NBG420N

Wireless N Router

User's Guide

Version 3.60
3/2008
Edition 1

DEFAULT LOGIN	
IP Address	**http://192.168.1.1**
Password	**1234**

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the NBG420N using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide
  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Supporting Disk
  Refer to the included CD for support documents.
- ZyXEL Web Site
  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

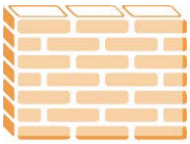
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The NBG420N may be referred to as the "NBG420N", the "device", the "product" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The NBG420N icon is not an exact representation of your device.

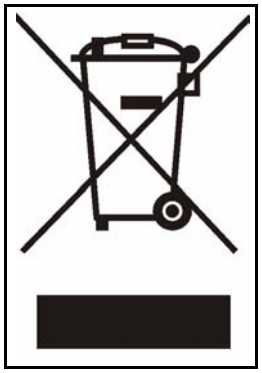
NBG420N	Computer	Notebook computer
Server	DSLAM	Firewall 
Telephone	Switch	Router
Modem		

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

This product is recyclable. Dispose of it properly.



Contents Overview

Introduction 29

Getting to Know Your NBG420N 31
The WPS Button 35
Introducing the Web Configurator 37
Connection Wizard 49
AP Mode 65
Tutorials 73

Network 87

Wireless LAN 89
WAN 117
LAN 127
DHCP 133
Network Address Translation (NAT) 137
Dynamic DNS 147

Security 151

Firewall 153
Content Filtering 161
IPSec VPN 165

Management 193

Static Route Screens 195
Bandwidth Management 199
Remote Management 209
Universal Plug-and-Play (UPnP) 215

Maintenance and Troubleshooting 227

System 229
Logs 233
Tools 251
Configuration Mode 257
Sys Op Mode 259
Language 263
Troubleshooting 265

Appendices and Index 271

Table of Contents

About This User's Guide **3**

Document Conventions **4**

Safety Warnings **6**

Contents Overview **9**

Table of Contents **11**

List of Figures **19**

List of Tables **25**

Part I: Introduction **29**

Chapter 1
Getting to Know Your NBG420N **31**

1.1 Overview 31
1.2 Router Mode 31
1.3 AP Mode 32
1.4 Router Features vs. AP Features 32
1.5 Ways to Manage the NBG420N 33
1.6 Good Habits for Managing the NBG420N 33
1.7 LEDs 33

Chapter 2
The WPS Button **35**

2.1 Overview 35

Chapter 3
Introducing the Web Configurator **37**

3.1 Web Configurator Overview 37
3.2 Accessing the Web Configurator 37
3.3 Resetting the NBG420N 39
3.3.1 Procedure to Use the Reset Button 39
3.4 Navigating the Web Configurator 39
3.5 The Status Screen in Router Mode 39
3.5.1 Navigation Panel 42

3.5.2 Summary: Any IP Table 44
3.5.3 Summary: Bandwidth Management Monitor 44
3.5.4 Summary: DHCP Table 45
3.5.5 Summary: Packet Statistics 46
3.5.6 Summary: VPN Monitor 47
3.5.7 Summary: Wireless Station Status 47

Chapter 4
Connection Wizard 49

4.1 Wizard Setup 49
4.2 Connection Wizard: STEP 1: System Information 50
4.2.1 System Name 50
4.2.2 Domain Name 51
4.3 Connection Wizard: STEP 2: Wireless LAN 51
4.3.1 Basic (WEP) Security 53
4.3.2 Extend (WPA-PSK or WPA2-PSK) Security 54
4.4 Connection Wizard: STEP 3: Internet Configuration 54
4.4.1 Ethernet Connection 55
4.4.2 PPPoE Connection 55
4.4.3 PPTP Connection 56
4.4.4 Your IP Address 58
4.4.5 WAN IP Address Assignment 58
4.4.6 IP Address and Subnet Mask 59
4.4.7 DNS Server Address Assignment 59
4.4.8 WAN IP and DNS Server Address Assignment 60
4.4.9 WAN MAC Address 61
4.5 Connection Wizard: STEP 4: Bandwidth management 62
4.6 Connection Wizard Complete 62

Chapter 5
AP Mode 65

5.1 AP Mode Overview 65
5.2 Setting your NBG420N to AP Mode 65
5.3 The Status Screen in AP Mode 66
5.3.1 Navigation Panel 68
5.4 Configuring Your Settings 69
5.4.1 LAN Settings 69
5.4.2 WLAN and Maintenance Settings 71
5.5 Logging in to the Web Configurator in AP Mode 71

Chapter 6
Tutorials 73

6.1 Wireless Tutorials 73

6.1.1 How to Connect to the Internet from an AP 73
6.1.2 Configure Wireless Security Using WPS on both your NBG420N and Wireless Client 73
6.1.3 Enable and Configure Wireless Security without WPS on your NBG420N 76
6.1.4 Configure Your Notebook 78
6.2 Site-To-Site VPN Tunnel Tutorial 80
6.2.1 Configuring Bob's NBG420N VPN Settings 81
6.2.2 Configuring Jack's NBG420N VPN Settings 83
6.2.3 Checking the VPN Connection 84

Part II: Network 87

Chapter 7
Wireless LAN 89

7.1 Wireless Network Overview 89
7.2 Wireless Security Overview 90
7.2.1 SSID 90
7.2.2 MAC Address Filter 90
7.2.3 User Authentication 90
7.2.4 Encryption 91
7.3 Roaming 92
7.3.1 Requirements for Roaming 93
7.4 Quality of Service 93
7.4.1 WMM QoS 94
7.5 General Wireless LAN Screen 94
7.5.1 No Security 96
7.5.2 WEP Encryption 96
7.5.3 WPA-PSK/WPA2-PSK 98
7.5.4 WPA/WPA2 99
7.6 MAC Filter 101
7.7 Wireless LAN Advanced Screen 102
7.8 Quality of Service (QoS) Screen 103
7.8.1 Application Priority Configuration 105
7.9 WiFi Protected Setup 106
7.9.1 WPS Screen 106
7.9.2 WPS Station Screen 107
7.9.3 Scheduling 107
7.10 iPod Touch Web Configurator 108
7.10.1 Login Screen 109
7.10.2 System Status 110
7.10.3 WPS in Progress 112
7.10.4 Port Forwarding 113

7.11 Accessing the iPod Touch Web Configurator 114
7.11.1 Accessing the iPod Touch Web Configurator 115

Chapter 8
WAN 117

8.1 WAN Overview 117
8.2 WAN MAC Address 117
8.3 Multicast 117
8.4 Internet Connection 118
8.4.1 Ethernet Encapsulation 118
8.4.2 PPPoE Encapsulation 119
8.4.3 PPTP Encapsulation 122
8.5 Advanced WAN Screen 125

Chapter 9
LAN 127

9.1 LAN Overview 127
9.1.1 IP Pool Setup 127
9.1.2 System DNS Servers 127
9.2 LAN TCP/IP 127
9.2.1 Factory LAN Defaults 127
9.2.2 IP Address and Subnet Mask 128
9.2.3 Multicast 128
9.2.4 Any IP 128
9.3 LAN IP Screen 130
9.4 LAN IP Alias 130
9.5 Advanced LAN Screen 131

Chapter 10
DHCP 133

10.1 DHCP 133
10.2 DHCP General Screen 133
10.3 DHCP Advanced Screen 134
10.4 Client List Screen 135

Chapter 11
Network Address Translation (NAT) 137

11.1 NAT Overview 137
11.2 Using NAT 137
11.2.1 Port Forwarding: Services and Port Numbers 137
11.2.2 Configuring Servers Behind Port Forwarding Example 138
11.3 General NAT Screen 138
11.4 NAT Application Screen 139

11.4.1 Game List Example 141
11.5 Trigger Port Forwarding 142
11.5.1 Trigger Port Forwarding Example 142
11.5.2 Two Points To Remember About Trigger Ports 143
11.6 NAT Advanced Screen 143

Chapter 12
Dynamic DNS 147

12.1 Dynamic DNS Introduction 147
12.1.1 DynDNS Wildcard 147
12.2 Dynamic DNS Screen 147

Part III: Security 151

Chapter 13
Firewall 153

13.1 Introduction to ZyXEL's Firewall 153
13.1.1 What is a Firewall? 153
13.1.2 Stateful Inspection Firewall 153
13.1.3 About the NBG420N Firewall 153
13.1.4 Guidelines For Enhancing Security With Your Firewall 154
13.2 Triangle Routes 154
13.2.1 Triangle Routes and IP Alias 154
13.3 General Firewall Screen 155
13.4 Services Screen 156
13.4.1 The Add Firewall Rule Screen 157

Chapter 14
Content Filtering 161

14.1 Introduction to Content Filtering 161
14.2 Restrict Web Features 161
14.3 Days and Times 161
14.4 Filter Screen 161
14.5 Schedule 163
14.6 Customizing Keyword Blocking URL Checking 164
14.6.1 Domain Name or IP Address URL Checking 164
14.6.2 Full Path URL Checking 164
14.6.3 File Name URL Checking 164

Chapter 15
IPSec VPN 165

15.1 IPSec VPN Overview 165
15.1.1 What You Can Do in the IPSec VPN Screens 165
15.1.2 What You Need To Know About IPSec VPN 166
15.1.3 IKE SA (IKE Phase 1) Overview 166
15.1.4 IPSec SA (IKE Phase 2) Overview 167
15.2 The General Screen 167
15.2.1 VPN Rule Setup (Basic) 168
15.2.2 VPN Rule Setup (Advanced) 173
15.2.3 VPN Rule Setup (Manual) 179
15.3 The SA Monitor Screen 183
15.4 VPN and Remote Management 184
15.5 IPSec VPN Technical Reference 185

Part IV: Management 193

Chapter 16
Static Route Screens 195

16.1 Static Route Overview 195
16.2 IP Static Route Screen 195
16.2.1 Static Route Setup Screen 196

Chapter 17
Bandwidth Management 199

17.1 Bandwidth Management Overview 199
17.2 Application-based Bandwidth Management 199
17.3 Subnet-based Bandwidth Management 199
17.4 Application and Subnet-based Bandwidth Management 200
17.5 Bandwidth Management Priorities 200
17.6 Predefined Bandwidth Management Services 201
17.6.1 Services and Port Numbers 201
17.7 Default Bandwidth Management Classes and Priorities 202
17.8 Bandwidth Management General Configuration 202
17.9 Bandwidth Management Advanced Configuration 203
17.9.1 Rule Configuration with the Pre-defined Service 205
17.9.2 Rule Configuration: User Defined Service Rule Configuration 205
17.10 Bandwidth Management Monitor 206

Chapter 18
Remote Management 209

18.1 Remote Management Overview 209
18.1.1 Remote Management Limitations 209

18.1.2 Remote Management and NAT 210
18.1.3 System Timeout 210
18.2 WWW Screen 210
18.3 Telnet 211
18.4 Telnet Screen 211
18.5 FTP Screen 212
18.6 DNS Screen 212

Chapter 19
Universal Plug-and-Play (UPnP) 215

19.1 Introducing Universal Plug and Play 215
19.1.1 How do I know if I'm using UPnP? 215
19.1.2 NAT Traversal 215
19.1.3 Cautions with UPnP 215
19.2 UPnP and ZyXEL 216
19.3 UPnP Screen 216
19.4 Installing UPnP in Windows Example 217

Part V: Maintenance and Troubleshooting 227

Chapter 20
System 229

20.1 System Overview 229
20.2 System General Screen 229
20.3 Time Setting Screen 230

Chapter 21
Logs 233

21.1 View Log 233
21.2 Log Settings 234
21.3 Log Descriptions 237

Chapter 22
Tools 251

22.1 Firmware Upload Screen 251
22.2 Configuration Screen 252
22.2.1 Backup Configuration 253
22.2.2 Restore Configuration 253
22.2.3 Back to Factory Defaults 254
22.3 Restart Screen 254
22.4 Wake On LAN 255

Chapter 23
Configuration Mode 257

Chapter 24
Sys Op Mode 259

24.1 Overview 259
24.1.1 Router 259
24.1.2 AP 259
24.2 Selecting System Operation Mode 260

Chapter 25
Language 263

25.1 Language Screen 263

Chapter 26
Troubleshooting 265

26.1 Power, Hardware Connections, and LEDs 265
26.2 NBG420N Access and Login 266
26.3 Internet Access 268
26.4 Resetting the NBG420N to Its Factory Defaults 269
26.5 Wireless Router/AP Troubleshooting 269
26.6 Advanced Features 270

Part VI: Appendices and Index 271

Appendix A Product Specifications and Wall-Mounting Instructions 273

Appendix B Pop-up Windows, JavaScripts and Java Permissions 279

Appendix C IP Addresses and Subnetting 285

Appendix D Setting up Your Computer's IP Address 293
26.6.1 Verifying Settings 308

Appendix E Wireless LANs 309
26.6.2 WPA(2)-PSK Application Example 318
26.6.3 WPA(2) with RADIUS Application Example 318

Appendix F Services 321

Appendix G Legal Information 325

Appendix H Customer Support 329

Index 335

List of Figures

Figure 1 Secure Wireless Internet Access in Router Mode 31
Figure 2 Wireless Internet Access in AP Mode 32
Figure 3 Front Panel 33
Figure 4 Change Password Screen 38
Figure 5 Selecting the setup mode 39
Figure 6 Web Configurator Status Screen 40
Figure 7 Any IP Table 44
Figure 8 Summary: BW MGMT Monitor 45
Figure 9 Summary: DHCP Table 45
Figure 10 Summary: Packet Statistics 46
Figure 11 Summary: VPN Monitor 47
Figure 12 Summary: Wireless Association List 47
Figure 13 Select Wizard or Advanced Mode 49
Figure 14 Select a Language 50
Figure 15 Welcome to the Connection Wizard 50
Figure 16 Wizard Step 1: System Information 51
Figure 17 Wizard Step 2: Wireless LAN 52
Figure 18 Wizard Step 2: Basic (WEP) Security 53
Figure 19 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security 54
Figure 20 Wizard Step 3: ISP Parameters. 55
Figure 21 Wizard Step 3: Ethernet Connection 55
Figure 22 Wizard Step 3: PPPoE Connection 56
Figure 23 Wizard Step 3: PPTP Connection 57
Figure 24 Wizard Step 3: Your IP Address 58
Figure 25 Wizard Step 3: WAN IP and DNS Server Addresses 60
Figure 26 Wizard Step 3: WAN MAC Address 61
Figure 27 Wizard Step 4: Bandwidth Management 62
Figure 28 Connection Wizard Save 63
Figure 29 Connection Wizard Complete 63
Figure 30 Wireless Internet Access in AP Mode 65
Figure 31 Maintenance > Sys OP Mode > General 66
Figure 32 Status: AP Mode 66
Figure 33 Menu: AP Mode 68
Figure 34 Network > LAN > IP 70
Figure 35 Wireless AP Connection to the Internet 73
Figure 36 Example WPS Process: PBC Method 75
Figure 37 Example WPS Process: PIN Method 76
Figure 38 Network > Wireless LAN > General 77

Figure 39 Status: AP Mode 78
Figure 40 Connecting a Wireless Client to a Wireless Network t 79
Figure 41 Security Settings 79
Figure 42 Confirm Save 79
Figure 43 Link Status 80
Figure 44 Site-To-Site VPN Tunnel 80
Figure 45 Property 81
Figure 46 Local Policy 81
Figure 47 Remote Policy 82
Figure 48 Authentication Method 82
Figure 49 IPSec Algorithm 82
Figure 50 VPN Summary 83
Figure 51 Property 83
Figure 52 Local Policy 83
Figure 53 Remote Policy 83
Figure 54 Authentication Method 84
Figure 55 IPSec Algorithm 84
Figure 56 VPN Summary 84
Figure 57 Pinging Jack's Local IP Address 85
Figure 58 SA Monitor 85
Figure 59 Example of a Wireless Network 89
Figure 60 Roaming Example 93
Figure 61 Network > Wireless LAN > General 95
Figure 62 Network > Wireless LAN > General: No Security 96
Figure 63 Network > Wireless LAN > General: Static WEP 97
Figure 64 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK 98
Figure 65 Network > Wireless LAN > General: WPA/WPA2 100
Figure 66 Network > Wireless LAN > MAC Filter 102
Figure 67 Network > Wireless LAN > Advanced 103
Figure 68 Network > Wireless LAN > QoS 104
Figure 69 Network > Wireless LAN > QoS: Application Priority Configuration 105
Figure 70 WPS 106
Figure 71 WPS Station 107
Figure 72 Scheduling 108
Figure 73 Login Screen 109
Figure 74 System Status screen 111
Figure 75 WPS In Progress 113
Figure 76 Port Forwarding 114
Figure 77 Login Screen 115
Figure 78 Network > WAN > Internet Connection: Ethernet Encapsulation 118
Figure 79 Network > WAN > Internet Connection: PPPoE Encapsulation 120
Figure 80 Network > WAN > Internet Connection: PPTP Encapsulation 123
Figure 81 Network > WAN > Advanced 125

Figure 82 Any IP Example 129
Figure 83 Network > LAN > IP 130
Figure 84 Network > LAN > IP Alias 131
Figure 85 Network > LAN > Advanced 131
Figure 86 Network > DHCP > General 133
Figure 87 Network > DHCP > Advanced 134
Figure 88 Network > DHCP > Client List 136
Figure 89 Multiple Servers Behind NAT Example 138
Figure 90 Network > NAT > General 138
Figure 91 Network > NAT > Application 140
Figure 92 Game List Example 142
Figure 93 Trigger Port Forwarding Process: Example 143
Figure 94 Network > NAT > Advanced 144
Figure 95 Dynamic DNS 148
Figure 96 Using IP Alias to Solve the Triangle Route Problem 155
Figure 97 Security > Firewall > General I 155
Figure 98 Security > Firewall > Services 156
Figure 99 Security > Firewall > Services > Adding a Rule 158
Figure 100 Security > Content Filter > Filter 162
Figure 101 Security > Content Filter > Schedule 163
Figure 102 IPSec VPN: Overview 165
Figure 103 VPN: IKE SA and IPSec SA 166
Figure 104 Security > VPN > General 167
Figure 105 IPSec Fields Summary 169
Figure 106 Security > VPN > General > Rule Setup: IKE (Basic) 169
Figure 107 Security > VPN > General > Rule Setup: IKE (Advanced) 174
Figure 108 Security > VPN > General > Rule Setup: Manual 180
Figure 109 Security > VPN > SA Monitor 183
Figure 110 VPN for Remote Management Example 184
Figure 111 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal 185
Figure 112 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange 185
Figure 113 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication 186
Figure 114 VPN/NAT Example 188
Figure 115 VPN: Transport and Tunnel Mode Encapsulation 189
Figure 116 Private DNS Server Example 191
Figure 117 Example of Static Routing Topology 195
Figure 118 Management > Static Route > IP Static Route 196
Figure 119 Management > Static Route > IP Static Route: Static Route Setup 197
Figure 120 Subnet-based Bandwidth Management Example 200
Figure 121 Management > Bandwidth MGMT > General 202
Figure 122 Management > Bandwidth MGMT > Advanced 203
Figure 123 Bandwidth Management Rule Configuration: Pre-defined Service 205
Figure 124 Management > Bandwidth MGMT > Advanced: User-defined Service Rule Configuration 206

Figure 125 Management > Bandwidth MGMT > Monitor 207
Figure 126 Management > Remote MGMT > WWW 210
Figure 127 Management > Remote MGMT > Telnet 211
Figure 128 Management > Remote MGMT > FTP 212
Figure 129 Management > Remote MGMT > DNS 213
Figure 130 Management > UPnP > General 216
Figure 131 Add/Remove Programs: Windows Setup: Communication 217
Figure 132 Add/Remove Programs: Windows Setup: Communication: Components 218
Figure 133 Network Connections 218
Figure 134 Windows Optional Networking Components Wizard 219
Figure 135 Networking Services 219
Figure 136 Network Connections 220
Figure 137 Internet Connection Properties 221
Figure 138 Internet Connection Properties: Advanced Settings 222
Figure 139 Internet Connection Properties: Advanced Settings: Add 222
Figure 140 System Tray Icon 223
Figure 141 Internet Connection Status 223
Figure 142 Network Connections 224
Figure 143 Network Connections: My Network Places 225
Figure 144 Network Connections: My Network Places: Properties: Example 225
Figure 145 Maintenance > System > General 229
Figure 146 Maintenance > System > Time Setting 230
Figure 147 Maintenance > Logs > View Log 233
Figure 148 Maintenance > Logs > Log Settings 235
Figure 149 Maintenance > Tools > Firmware 251
Figure 150 Upload Warning 252
Figure 151 Network Temporarily Disconnected 252
Figure 152 Upload Error Message 252
Figure 153 Maintenance > Tools > Configuration 253
Figure 154 Configuration Restore Successful 254
Figure 155 Temporarily Disconnected 254
Figure 156 Configuration Restore Error 254
Figure 157 Maintenance > Tools > Restart 255
Figure 158 Maintenance > Tools > Wake On LAN 255
Figure 159 Maintenance > Config Mode > General 257
Figure 160 LAN and WAN IP Addresses in Router Mode 259
Figure 161 IP Address in AP Mode 260
Figure 162 Maintenance > Sys OP Mode > General 260
Figure 163 Maintenance > Sys Op Mode > General: Router 260
Figure 164 Maintenance > Sys Op Mode > General: AP 261
Figure 165 Language 263
Figure 166 Wall-mounting Example 277
Figure 167 Masonry Plug and M4 Tap Screw 278

Figure 168 Pop-up Blocker 279
Figure 169 Internet Options: Privacy 280
Figure 170 Internet Options: Privacy 281
Figure 171 Pop-up Blocker Settings 281
Figure 172 Internet Options: Security 282
Figure 173 Security Settings - Java Scripting 283
Figure 174 Security Settings - Java 283
Figure 175 Java (Sun) 284
Figure 176 Network Number and Host ID 286
Figure 177 Subnetting Example: Before Subnetting 288
Figure 178 Subnetting Example: After Subnetting 289
Figure 179 WIndows 95/98/Me: Network: Configuration 294
Figure 180 Windows 95/98/Me: TCP/IP Properties: IP Address 295
Figure 181 Windows 95/98/Me: TCP/IP Properties: DNS Configuration 296
Figure 182 Windows XP: Start Menu 297
Figure 183 Windows XP: Control Panel 297
Figure 184 Windows XP: Control Panel: Network Connections: Properties 298
Figure 185 Windows XP: Local Area Connection Properties 298
Figure 186 Windows XP: Internet Protocol (TCP/IP) Properties 299
Figure 187 Windows XP: Advanced TCP/IP Properties 300
Figure 188 Windows XP: Internet Protocol (TCP/IP) Properties 301
Figure 189 Macintosh OS 8/9: Apple Menu 302
Figure 190 Macintosh OS 8/9: TCP/IP 302
Figure 191 Macintosh OS X: Apple Menu 303
Figure 192 Macintosh OS X: Network 304
Figure 193 Red Hat 9.0: KDE: Network Configuration: Devices 305
Figure 194 Red Hat 9.0: KDE: Ethernet Device: General 306
Figure 195 Red Hat 9.0: KDE: Network Configuration: DNS 306
Figure 196 Red Hat 9.0: KDE: Network Configuration: Activate 307
Figure 197 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 307
Figure 198 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 307
Figure 199 Red Hat 9.0: DNS Settings in resolv.conf 308
Figure 200 Red Hat 9.0: Restart Ethernet Card 308
Figure 201 Red Hat 9.0: Checking TCP/IP Properties 308
Figure 202 Peer-to-Peer Communication in an Ad-hoc Network 309
Figure 203 Basic Service Set 310
Figure 204 Infrastructure WLAN 311
Figure 205 RTS/CTS 312
Figure 206 WPA(2)-PSK Authentication 318

List of Tables

Table 1 Features Available in Router Mode vs. AP Mode 32
Table 2 Front Panel LEDs 33
Table 3 Status Screen Icon Key 40
Table 4 Web Configurator Status Screen 40
Table 5 Screens Summary 42
Table 6 Summary: DHCP Table 45
Table 7 Summary: Packet Statistics 46
Table 8 Summary: Wireless Association List 47
Table 9 Summary: Wireless Association List 48
Table 10 Wizard Step 1: System Information 51
Table 11 Wizard Step 2: Wireless LAN 52
Table 12 Wizard Step 2: Basic (WEP) Security 53
Table 13 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security 54
Table 14 Wizard Step 3: ISP Parameters 55
Table 15 Wizard Step 3: PPPoE Connection 56
Table 16 Wizard Step 3: PPTP Connection 57
Table 17 Wizard Step 3: Your IP Address 58
Table 18 Private IP Address Ranges 58
Table 19 Wizard Step 3: WAN IP and DNS Server Addresses 60
Table 20 Example of Network Properties for LAN Servers with Fixed IP Addresses 61
Table 21 Wizard Step 3: WAN MAC Address 61
Table 22 Wizard Step 4: Bandwidth Management 62
Table 23 Web Configurator Status Screen 67
Table 24 Screens Summary 68
Table 25 Network > LAN > IP 70
Table 26 Site-To-Site VPN Tunnel Settings 80
Table 27 Types of Encryption for Each Type of Authentication 91
Table 28 WMM QoS Priorities 94
Table 29 Network > Wireless LAN > General 95
Table 30 Wireless No Security 96
Table 31 Network > Wireless LAN > General: Static WEP 97
Table 32 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK 99
Table 33 Network > Wireless LAN > General: WPA/WPA2 100
Table 34 Network > Wireless LAN > MAC Filter 102
Table 35 Network > Wireless LAN > Advanced 103
Table 36 Network > Wireless LAN > QoS 104
Table 37 WPS 106
Table 38 WPS Station 107

Table 39 Scheduling 108
Table 40 Login Screen 109
Table 41 System Status screen 111
Table 42 Port Forwarding 114
Table 43 Network > WAN > Internet Connection: Ethernet Encapsulation 119
Table 44 Network > WAN > Internet Connection: PPPoE Encapsulation 121
Table 45 Network > WAN > Internet Connection: PPTP Encapsulation 123
Table 46 WAN > Advanced 125
Table 47 Network > LAN > IP 130
Table 48 Network > LAN > IP Alias 131
Table 49 Network > LAN > Advanced 132
Table 50 Network > DHCP > General 133
Table 51 Network > DHCP > Advanced 134
Table 52 Network > DHCP > Client List 136
Table 53 Network > NAT > General 139
Table 54 NAT Application 140
Table 55 Network > NAT > Advanced 144
Table 56 Dynamic DNS 148
Table 57 Security > Firewall > General 155
Table 58 Security > Firewall > Services 156
Table 59 Security > Firewall > Services > Adding a Rule 158
Table 60 Security > Content Filter > Filter 162
Table 61 Security > Content Filter > Schedule 163
Table 62 Security > VPN > General 168
Table 63 SECURITY > VPN > Rule Setup: IKE (Basic) 170
Table 64 Security > VPN > Rule Setup: IKE (Advanced) 175
Table 65 Security > VPN > Rule Setup: Manual 180
Table 66 Security > VPN > SA Monitor 184
Table 67 VPN Example: Matching ID Type and Content 186
Table 68 VPN Example: Mismatching ID Type and Content 187
Table 69 Management > Static Route > IP Static Route 196
Table 70 Management > Static Route > IP Static Route: Static Route Setup 197
Table 71 Application and Subnet-based Bandwidth Management Example 200
Table 72 Bandwidth Management Priorities 200
Table 73 Media Bandwidth Management Setup: Services 201
Table 74 Bandwidth Management Priority with Default Classes 202
Table 75 Management > Bandwidth MGMT > General 203
Table 76 Management > Bandwidth MGMT > Advanced 204
Table 77 Bandwidth Management Rule Configuration: Pre-defined Service 205
Table 78 Management > Bandwidth MGMT > Advanced: User-defined Service Rule Configuration 206
Table 79 Management > Remote MGMT > WWW 210
Table 80 Management > Remote MGMT > Telnet 211
Table 81 Management > Remote MGMT > FTP 212

Table 82 Management > Remote MGMT > DNS 213
Table 83 Management > UPnP > General 216
Table 84 Maintenance > System > General 229
Table 85 Maintenance > System > Time Setting 231
Table 86 Maintenance > Logs > View Log 234
Table 87 Maintenance > Logs > Log Settings 235
Table 88 System Maintenance Logs 237
Table 89 System Error Logs 238
Table 90 Access Control Logs 238
Table 91 TCP Reset Logs 238
Table 92 Packet Filter Logs 239
Table 93 ICMP Logs 239
Table 94 CDR Logs 240
Table 95 PPP Logs 240
Table 96 UPnP Logs 240
Table 97 Content Filtering Logs 240
Table 98 Attack Logs 241
Table 99 IPSec Logs 242
Table 100 IKE Logs 242
Table 101 PKI Logs 245
Table 102 802.1X Logs 246
Table 103 ACL Setting Notes 247
Table 104 ICMP Notes 247
Table 105 Syslog Logs 248
Table 106 RFC-2408 ISAKMP Payload Types 249
Table 107 Maintenance > Tools > Firmware 251
Table 108 Maintenance Restore Configuration 253
Table 109 Maintenance > Tools > Wake On LAN 255
Table 110 Maintenance > Config Mode > General 257
Table 111 Advanced Configuration Options 258
Table 112 Maintenance > Sys OP Mode > General 261
Table 113 Hardware Features 273
Table 114 Firmware Features 274
Table 115 Feature Specifications 275
Table 116 Standards Supported 276
Table 117 Subnet Mask - Identifying Network Number 286
Table 118 Subnet Masks 287
Table 119 Maximum Host Numbers 287
Table 120 Alternative Subnet Mask Notation 287
Table 121 Subnet 1 289
Table 122 Subnet 2 290
Table 123 Subnet 3 290
Table 124 Subnet 4 290

Table 125 Eight Subnets 290
Table 126 24-bit Network Number Subnet Planning 291
Table 127 16-bit Network Number Subnet Planning 291
Table 128 IEEE 802.11g 313
Table 129 Comparison of EAP Authentication Types 316
Table 130 Wireless Security Relational Matrix 319
Table 131 Examples of Services 321

PART I
Introduction

Getting to Know Your NBG420N (31)
The WPS Button (35)
Introducing the Web Configurator (37)
Connection Wizard (49)
AP Mode (65)
Tutorials (73)

1

Getting to Know Your NBG420N

This chapter introduces the main features and applications of the NBG420N.

1.1 Overview

The NBG420N acts as either an access point (AP) or a secure broadband router for all data passing between the Internet and your local network. In both **AP** and **Router Mode** you can set up a wireless network with other IEEE 802.11b/g/n compatible devices. In **Router Mode** a number of services such as a firewall, IPSec VPN and content filtering are also available. You can use media bandwidth management to efficiently manage traffic on your network. Bandwidth management features allow you to prioritize time-sensitive or highly important applications such as Voice over the Internet (VoIP).

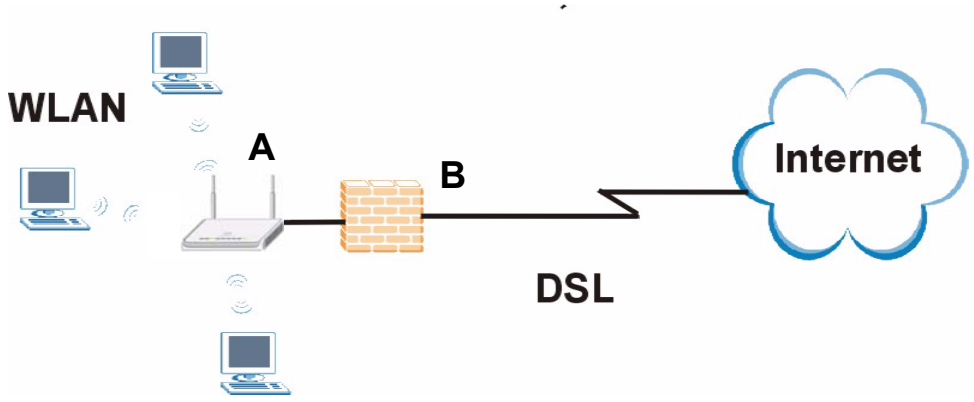
The NBG420N also uses MIMO (Multiple-In, Multiple-Out) antenna technology to deliver high-speed wireless networking.

1.2 Router Mode

Select **Router Mode** if you need to route traffic between your network and another network such as the Internet, and require important network services such as a firewall or bandwidth management.

The following figure shows computers in a WLAN connecting to the NBG420N (**A**), which has a DSL connection to the Internet. The NBG420N is set to **Router Mode** and has router features such as a built-in firewall (**B**).

Figure 1 Secure Wireless Internet Access in Router Mode

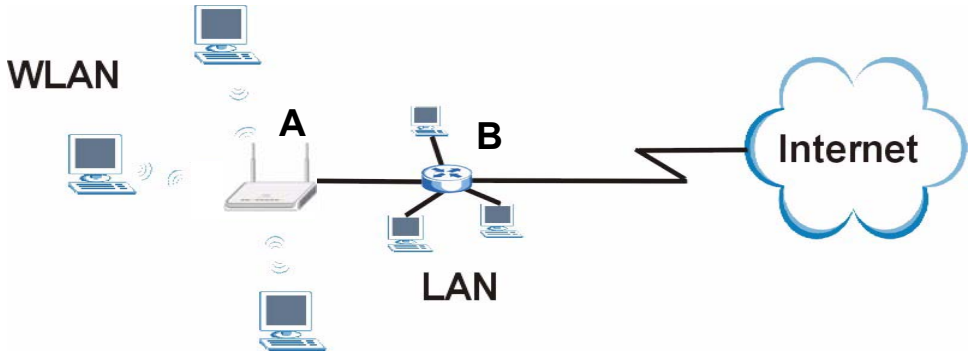


1.3 AP Mode

Select **AP Mode** if you already have a router or gateway on your network which provides network services such as a firewall or bandwidth management.

The following figure shows computers in a WLAN connecting to the NBG420N, which acts as an access point (**A**). The NBG420N allows the wireless computers to share the same Internet access as the other computers connected to the router (**B**) on the same network.

Figure 2 Wireless Internet Access in AP Mode



1.4 Router Features vs. AP Features

The following table shows which features are available in **Router** or **AP Mode**.

Table 1 Features Available in Router Mode vs. AP Mode

FEATURE	ROUTER MODE	AP MODE
DHCP This allows individual clients to obtain IP addresses at start-up from a DHCP server.	YES	NO
Firewall This establishes a network security barrier, protecting your network from attacks and controlling access between your network and the Internet.	YES	NO
Bandwidth Management This allows you to allocate network bandwidth to specific applications and or subnets.	YES	NO
Any IP This allows a computer to access the NBG420N when the IP addresses of the computer and the NBG420N are not in the same subnet.)	YES	NO
VPN A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines.	YES	NO
Wireless This allows two or more devices to communicate without wires, based on IEEE 802.11 wireless standards.	YES	YES

1.5 Ways to Manage the NBG420N

Use any of the following methods to manage the NBG420N.

- Web Configurator. This is recommended for everyday management of the NBG420N using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup/restore.

1.6 Good Habits for Managing the NBG420N

Do the following things regularly to make the NBG420N more secure and to manage the NBG420N more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the NBG420N to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the NBG420N. You could simply restore your last configuration.

1.7 LEDs

Figure 3 Front Panel

The following table describes the LEDs.

Table 2 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The NBG420N is receiving power and functioning properly.
		Off	The NBG420N is not receiving power.

Table 2 Front Panel LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
LAN 1-4	Green	On	The NBG420N has a successful 10MB Ethernet connection.
		Blinking	The NBG420N is sending/receiving data.
	Amber	On	The NBG420N has a successful 100MB Ethernet connection.
		Blinking	The NBG420N is sending/receiving data.
		Off	The LAN is not connected.
WAN	Green	On	The NBG420N has a successful 10MB WAN connection.
		Blinking	The NBG420N is sending/receiving data.
	Amber	On	The NBG420N has a successful 100MB Ethernet connection.
		Blinking	The NBG420N is sending/receiving data.
		Off	The WAN connection is not ready, or has failed.
WLAN	Green	On	The NBG420N is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The NBG420N is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
WPS	Green	On	WPS (WiFi Protected Setup) is configured on your device.
		Blinking	The NBG420N is attempting to connect with another wireless devices using WPS.
		Off	WPS is disabled on your device.

2

The WPS Button

2.1 Overview

Your NBG420N supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

For more information on using WPS, see Section 6.1.2 on page 73.

3

Introducing the Web Configurator

This chapter describes how to access the NBG420N web configurator and provides an overview of its screens.

3.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy setup and management of the NBG420N via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions or Safari 2.0 or later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter to see how to make sure these functions are allowed in Internet Explorer.

3.2 Accessing the Web Configurator

1. Make sure your NBG420N hardware is properly connected and prepare your computer or computer network to connect to the NBG420N (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "http://192.168.1.1" as the website address.

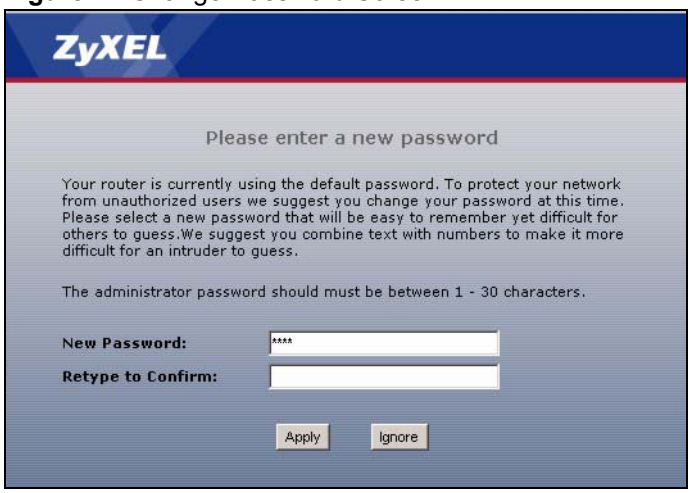
Your computer must be in the same subnet in order to access this website address.

- In **Router Mode** enable the DHCP Server. The NBG420N assigns your computer an IP address on the same subnet.
- In **AP Mode** the NBG420N does not assign an IP address to your computer, so you should check it's in the same subnet. See Section 5.5 on page 71 for more information.

4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 4 Change Password Screen


ZyXEL
Please enter a new password
Your router is currently using the default password. To protect your network from unauthorized users we suggest you change your password at this time. Please select a new password that will be easy to remember yet difficult for others to guess.We suggest you combine text with numbers to make it more difficult for an intruder to guess.
The administrator password should must be between 1 - 30 characters.
New Password:
****
Retype to Confirm:
Apply
Ignore

The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the NBG420N if this happens.

6 Select the setup mode you want to use.

- Click **Go to Wizard Setup** to use the Configuration Wizard for basic Internet and Wireless setup.
- Click **Go to Basic Setup** if you want to view and configure basic settings that are not part of the wizard setup. Not all Web Configurator screens are available in this mode. See Chapter 23 on page 257 for more information.
- **Click Go to Advanced Setup** to view and configure all the NBG420N's settings.
- Select a language to go to the basic web configurator in that language. To change to the advanced configurator see Chapter 23 on page 257.

Figure 5 Selecting the setup mode

ZyXEL
Please select Wizard, Basic, or Advanced mode
The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router.
Use Basic mode if you need to make basic configuration changes.
Use Advanced mode if you need access to more advanced features.
Go to Wizard setup
Go to Basic setup
Go to Advanced setup
Please choose the language you need
English
Deutsch
Français
Español
繁體中文
Italiano
Exit

3.3 Resetting the NBG420N

If you forget your password or IP address, or you cannot access the web configurator, you will need to use the **RESET** button at the back of the NBG420N to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to "1234" and the IP address will be reset to "192.168.1.1".

3.3.1 Procedure to Use the Reset Button

1. Make sure the power LED is on.
2. Press the **RESET** button for five seconds or until the power LED begins to blink and then release it. When the power LED begins to blink, the defaults have been restored and the NBG420N restarts.

3.4 Navigating the Web Configurator

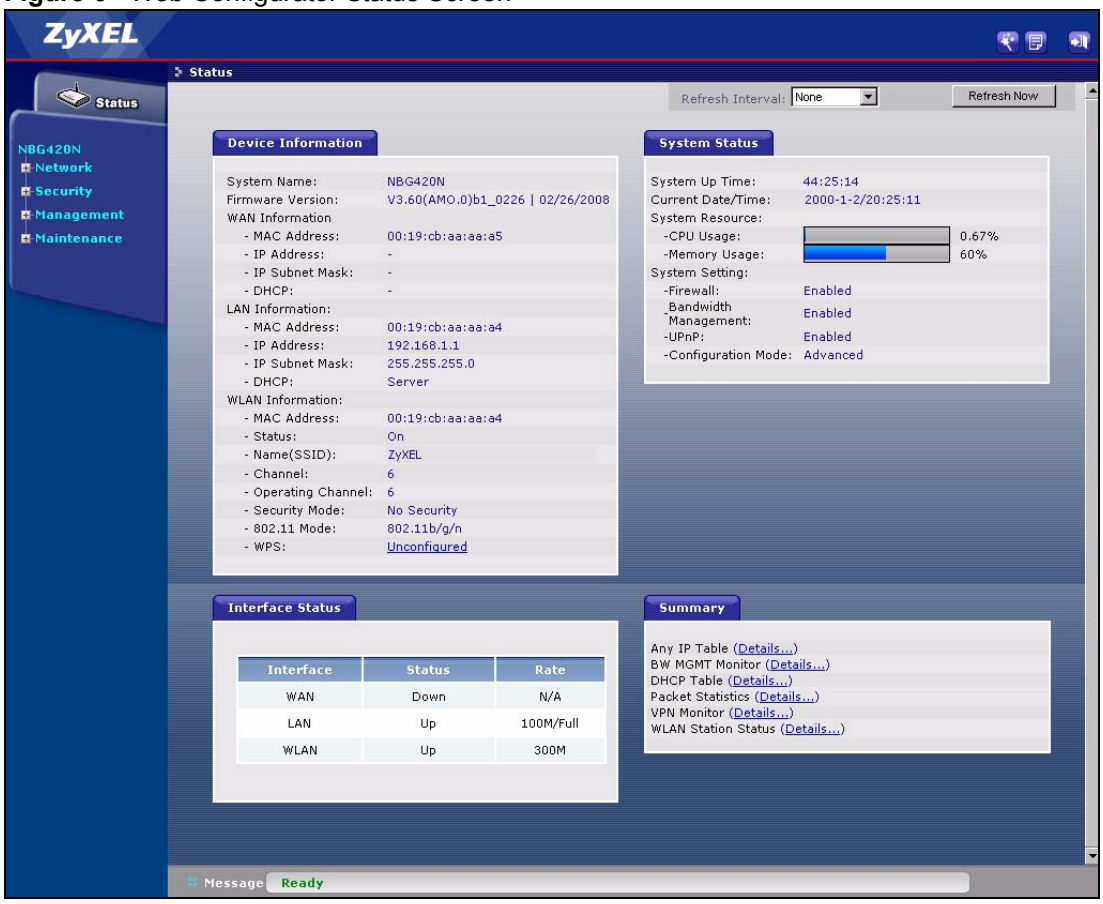
The following summarizes how to navigate the web configurator from the **Status** screen in **Router Mode** and **AP Mode**.

3.5 The Status Screen in Router Mode

Click on **Status**. The screen below shows the status screen in **Router Mode**.

(For information on the status screen in **AP Mode** see Chapter 5 on page 66.)

Figure 6 Web Configurator Status Screen



The following table describes the icons shown in the **Status** screen.

Table 3 Status Screen Icon Key

ICON	DESCRIPTION
	Click this icon to open the setup wizard.
	Click this icon to view copyright and a link for related product information.
	Click this icon at any time to exit the web configurator.
	Select a number of seconds or **None** from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
	Click this button to refresh the status screen statistics.

The following table describes the labels shown in the **Status** screen.

Table 4 Web Configurator Status Screen

LABEL	DESCRIPTION
Device Information	
System Name	This is the **System Name** you enter in the **Maintenance** > **System** > **General** screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.

Table 4 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
WAN Information	
- MAC Address	This shows the WAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the WAN port's IP address.
- IP Subnet Mask	This shows the WAN port's subnet mask.
- DHCP	This shows the WAN port's DHCP role - **Client** or **None**.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - **Server** or **None**.
WLAN Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - **On**, **Off** or **Off by scheduler**.
- Name (SSID)	This shows a descriptive name used to identify the NBG420N in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the NBG420N is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG420N is using.
- 802.11 Mode	This shows the wireless standard.
- WPS	This displays **Configured** when the WPS has been set up. This displays **Unconfigured** if the WPS has not been set up. Click the status to display Network > Wireless LAN > WPS screen.
System Status	
System Up Time	This is the total time the NBG420N has been on.
Current Date/Time	This field displays your NBG420N's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG420N's processing ability is currently used. When this percentage is close to 100%, the NBG420N is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.
- Memory Usage	This shows what percentage of the heap memory the NBG420N is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT and the firewall.
System Setting	
- Firewall	This shows whether the firewall is active or not.
- Bandwidth Management	This shows whether the bandwidth management is active or not.
- UPnP	This shows whether UPnP is active or not.
- Configuration Mode	This shows whether the advanced screens of each feature are turned on (**Advanced**) or not (**Basic**).
Interface Status	
Interface	This displays the NBG420N port types. The port types are: **WAN**, **LAN** and **WLAN**.

Table 4 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
Status	For the LAN and WAN ports, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.
Rate	For the LAN ports, this displays the port speed and duplex setting or **N/A** when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
Summary	
Any IP Table	Use this screen to view details of IP addresses assigned to devices not in the same subnet as the NBG420N.
BW MGMT Monitor	Use this screen to view the NBG420N's bandwidth usage and allotments.
DHCP Table	Use this screen to view current DHCP client information.
Packet Statistics	Use this screen to view port status and packet specific statistics.
VPN Monitor	Use this screen to view the active VPN connections.
WLAN Station Status	Use this screen to view the wireless stations that are currently associated to the NBG420N.

3.5.1 Navigation Panel

Use the sub-menus on the navigation panel to configure NBG420N features.

The following table describes the sub-menus.

Table 5 Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the NBG420N's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG420N to block access to devices or block the devices from accessing the NBG420N.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
WAN	Internet Connection	This screen allows you to configure ISP parameters, WAN IP address assignment, DNS servers and the WAN MAC address.
	Advanced	Use this screen to configure other advanced properties.

Table 5 Screens Summary

LINK	TAB	FUNCTION
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
	IP Alias	Use this screen to partition your LAN interface into subnets.
	Advanced	Use this screen to enable other advanced properties.
DHCP Server	General	Use this screen to enable the NBG420N's DHCP server.
	Advanced	Use this screen to assign IP addresses to specific individual computers based on their MAC addresses and to have DNS servers assigned by the DHCP server.
	Client List	Use this screen to view current DHCP client information and to always assign an IP address to a MAC address (and host name).
NAT	General	Use this screen to enable NAT.
	Application	Use this screen to configure servers behind the NBG420N.
	Advanced	Use this screen to change your NBG420N's port triggering settings.
DDNS	General	Use this screen to set up dynamic DNS.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
Content Filter	Filter	Use this screen to block certain web features and sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for the NBG420N to perform content filtering.
VPN	General	Use this screen to configure VPN connections and view the rule summary.
	SA Monitor	Use this screen to display and manage active VPN connections.
Management		
Static Route	IP Static Route	Use this screen to configure IP static routes.
Bandwidth MGMT	General	Use this screen to enable bandwidth management.
	Advanced	Use this screen to set the upstream bandwidth and edit a bandwidth management rule.
	Monitor	Use this screen to view the NBG420N's bandwidth usage and allotments.
Remote MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the NBG420N.
	Telnet	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the NBG420N.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the NBG420N.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the NBG420N.
UPnP	General	Use this screen to enable UPnP on the NBG420N.
Maintenance		

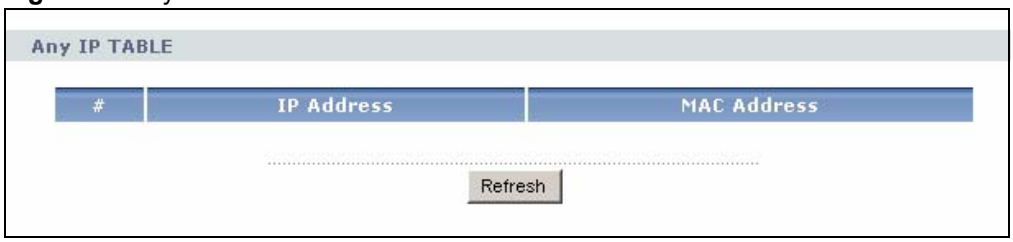
Table 5 Screens Summary

LINK	TAB	FUNCTION
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	Time Setting	Use this screen to change your NBG420N's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your NBG420N's log settings.
Tools	Firmware	Use this screen to upload firmware to your NBG420N.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG420N.
	Restart	This screen allows you to reboot the NBG420N without turning the power off.
	Wake On LAN	Use this screen to remotely turn on a device on the network.
Config Mode	General	This screen allows you to display or hide the advanced screens or features.
Sys OP Mode	General	This screen allows you to select whether your device acts as a Router or a Access Point.
Language		This screen allows you to select the language you prefer.

3.5.2 Summary: Any IP Table

This screen displays the IP address of each computer that is using the NBG420N via the any IP feature. Any IP allows computers to access the Internet through the NBG420N without changing their network settings when NAT is enabled. To access this screen, open the **Status** screen (see Section 3.5 on page 39), and click **(Details...)** next to **Any IP Table**.

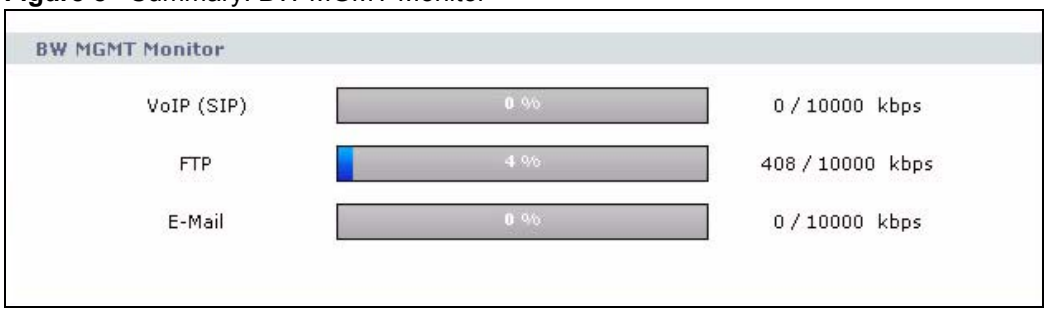
Figure 7 Any IP Table



3.5.3 Summary: Bandwidth Management Monitor

Select the **BW MGMT Monitor (Details...)** hyperlink in **Status** screen. View the bandwidth usage of the WAN configured bandwidth rules. This is also shown as bandwidth usage over the bandwidth budget for each rule. The gray section of the bar represents the percentage of unused bandwidth and the blue color represents the percentage of bandwidth in use.

Figure 8 Summary: BW MGMT Monitor

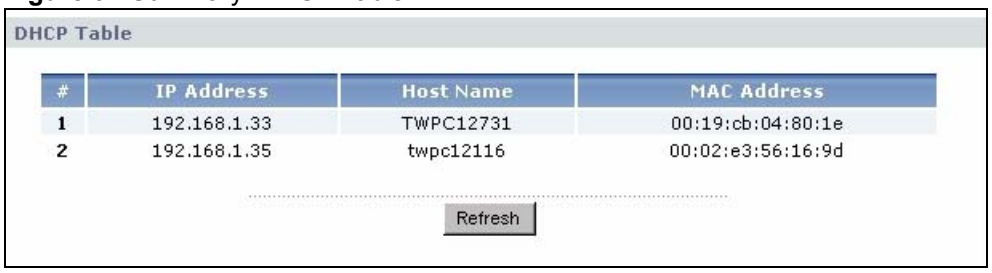


3.5.4 Summary: DHCP Table

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the NBG420N's LAN as a DHCP server or disable it. When configured as a server, the NBG420N provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on that network, or else the computer must be manually configured.

Click the **DHCP Table (Details...)** hyperlink in the **Status** screen. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the NBG420N's DHCP server.

Figure 9 Summary: DHCP Table



The following table describes the labels in this screen.

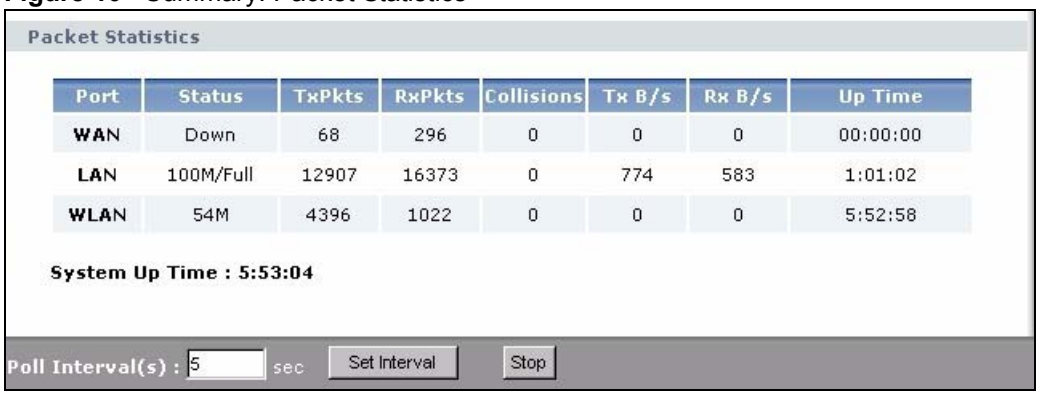
Table 6 Summary: DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click **Refresh** to renew the screen.

3.5.5 Summary: Packet Statistics

Click the **Packet Statistics (Details...)** hyperlink in the **Status** screen. Read-only information here includes port status, packet specific statistics and the "system up time". The **Poll Interval(s)** field is configurable and is used for refreshing the screen.

Figure 10 Summary: Packet Statistics



The following table describes the labels in this screen.

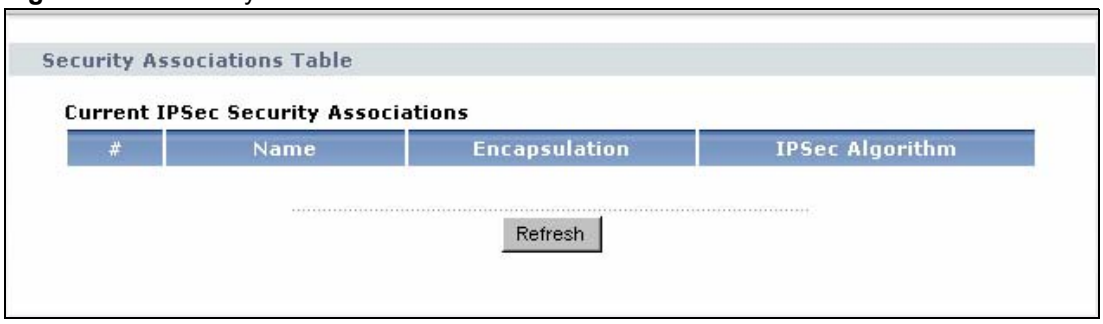
Table 7 Summary: Packet Statistics

LABEL	DESCRIPTION
Port	This is the NBG420N's port type.
Status	For the LAN ports, this displays the port speed and duplex setting or **Down** when the line is disconnected. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE or PPTP encapsulation. This field displays **Down** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **Down** when the WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the NBG420N has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

3.5.6 Summary: VPN Monitor

Click the **VPN Monitor (Details...)** hyperlink in the **Status** screen. This screen displays read-only information about the active VPN connections. Click the **Refresh** button to update the screen. A Security Association (SA) is the group of security settings related to a specific VPN tunnel.

Figure 11 Summary: VPN Monitor



The following table describes the labels in this screen.

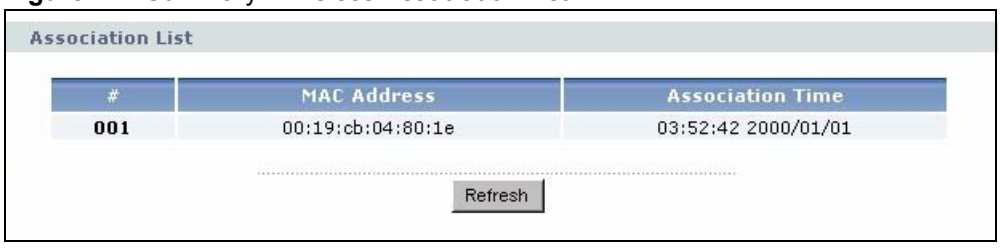
Table 8 Summary: Wireless Association List

LABEL	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN tunnel.
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase NBG420N processing requirements and communications latency (delay).
Refresh	Click this button to update the screen's statistics immediately.

3.5.7 Summary: Wireless Station Status

Click the **WLAN Station Status (Details...)** hyperlink in the **Status** screen. View the wireless stations that are currently associated to the NBG420N in the **Association List**. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Figure 12 Summary: Wireless Association List



The following table describes the labels in this screen.

Table 9 Summary: Wireless Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the NBG420N's WLAN network.
Refresh	Click **Refresh** to reload the list.

4

Connection Wizard

This chapter provides information on the wizard setup screens in the web configurator.

4.1 Wizard Setup

The web configurator's wizard setup helps you configure your device to access the Internet. Refer to your ISP (Internet Service Provider) checklist in the Quick Start Guide to know what to enter in each field. Leave a field blank if you don't have that information.

1 After you access the NBG420N web configurator, click the **Go to Wizard setup** hyperlink.

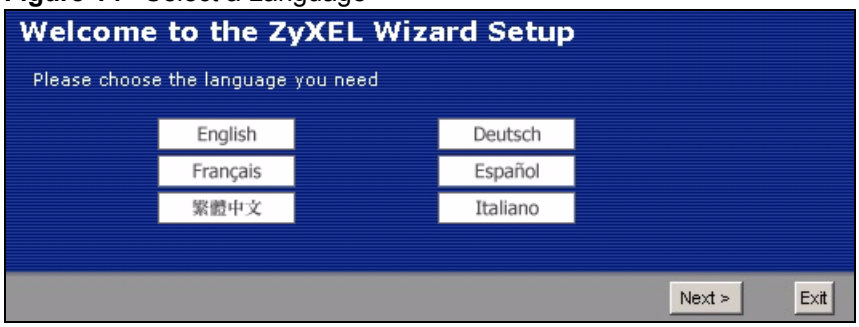
You can click the **Go to Basic setup** or **Go to Advanced setup** hyperlink to skip this wizard setup and configure basic or advanced features accordingly.

Figure 13 Select Wizard or Advanced Mode

ZyXEL
Please select Wizard, Basic, or Advanced mode
The Wizard setup walks you through the most common configuration settings. We suggest you use this mode if it is the first time you are setting up your router.
Use Basic mode if you need to make basic configuration changes.
Use Advanced mode if you need access to more advanced features.
Go to Wizard setup
Go to Basic setup
Go to Advanced setup
Please choose the language you need
English
Deutsch
Français
Español
繁體中文
Italiano
Exit

2 Choose a language by clicking on the language's button. The screen will update. Click the **Next** button to proceed to the next screen.

Figure 14 Select a Language



3 Read the on-screen information and click **Next**.

Figure 15 Welcome to the Connection Wizard

Welcome to the ZyXEL Connection Wizard
The Connection Wizard will walk you through the most common configuration options. This wizard has been broken down into three steps, each of which may have multiple pages.
This wizard will take you through the following steps:
Step 1 : System Information Setup.
Step 2 : Wireless LAN Setup.
Step 3 : Internet Configuration Setup.
Step 4 : Bandwidth Management Setup.
<Back
Next >
Exit

4.2 Connection Wizard: STEP 1: System Information

System Information contains administrative and system-related information.

4.2.1 System Name

System Name is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

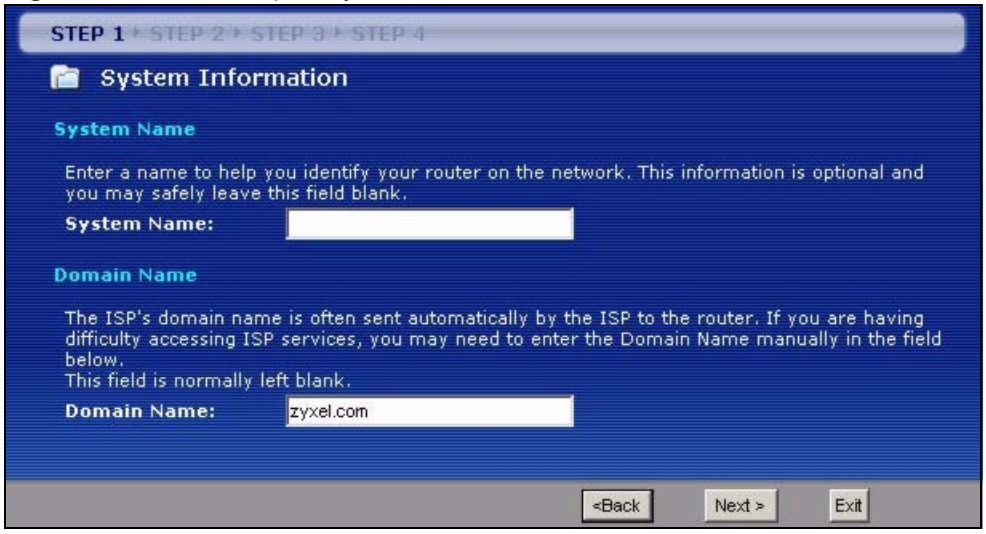
- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings** and **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the NBG420N **System Name**.

4.2.2 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the NBG420N via DHCP.

Click **Next** to configure the NBG420N for Internet access.

Figure 16 Wizard Step 1: System Information


STEP 1 STEP 2 STEP 3 STEP 4
System Information
System Name
Enter a name to help you identify your router on the network. This information is optional and you may safely leave this field blank.
System Name:
Domain Name
The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.
This field is normally left blank.
Domain Name:
zyxel.com
<Back
Next >
Exit

The following table describes the labels in this screen.

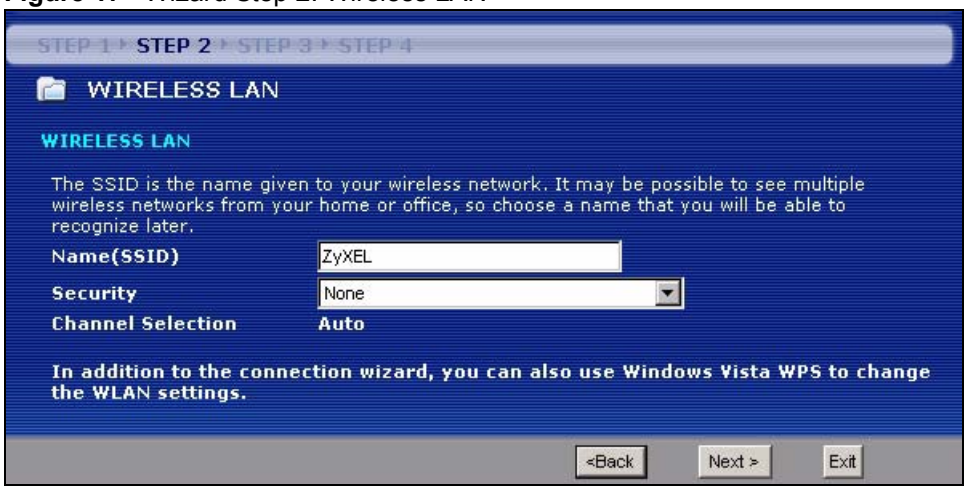
Table 10 Wizard Step 1: System Information

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the NBG420N in an Ethernet network. Enter a descriptive name. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Type the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

4.3 Connection Wizard: STEP 2: Wireless LAN

Set up your wireless LAN using the following screen.

Figure 17 Wizard Step 2: Wireless LAN


STEP 1 STEP 2 STEP 3 STEP 4
WIRELESS LAN
WIRELESS LAN
The SSID is the name given to your wireless network. It may be possible to see multiple wireless networks from your home or office, so choose a name that you will be able to recognize later.
Name(SSID)
ZyXEL
Security
None
Channel Selection
Auto
In addition to the connection wizard, you can also use Windows Vista WPS to change the WLAN settings.
<Back
Next >
Exit

The following table describes the labels in this screen.

Table 11 Wizard Step 2: Wireless LAN

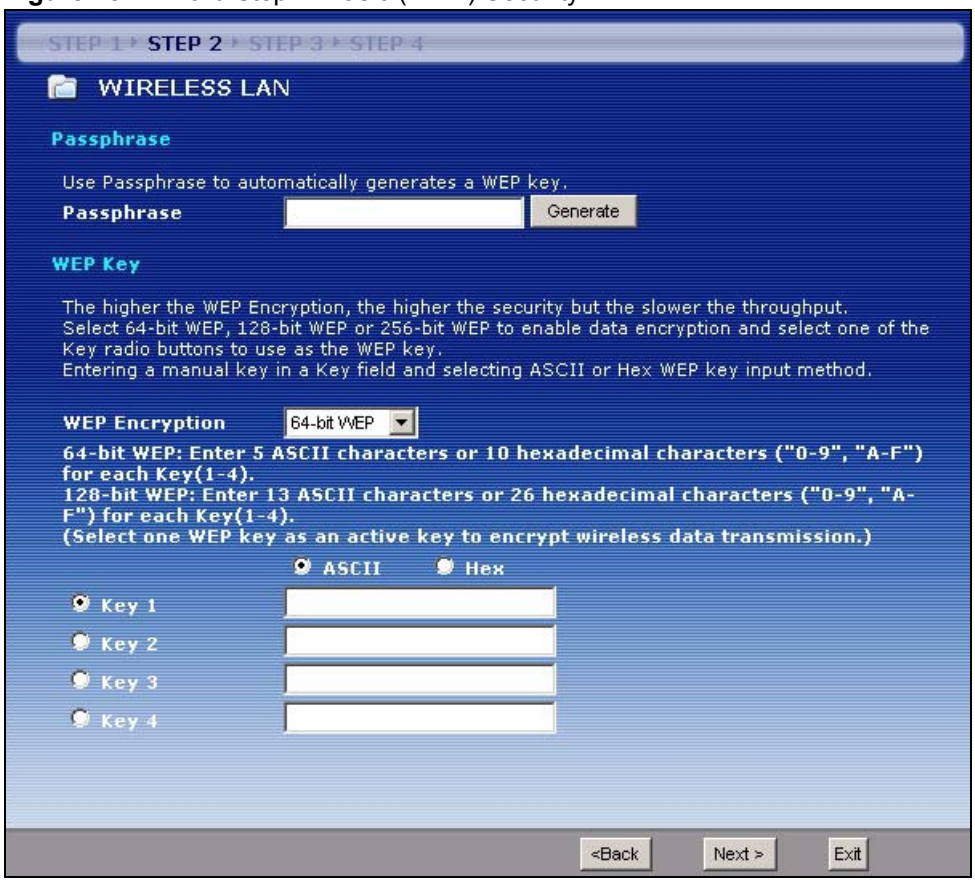
LABEL	DESCRIPTION
Name (SSID)	Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. If you change this field on the NBG420N, make sure all wireless stations use the same SSID in order to access the network.
Security	Select a **Security** level from the drop-down list box. Choose **Auto (WPA2-PSK)** to have the NBG420N generate a pre-shared key automatically. After you click **Next** a screen pops up displaying the generated pre-shared key. Write down the key for use later when connecting other wireless devices to your network. Click **OK** to continue. Choose **None** to have no wireless LAN security configured. If you do not enable any wireless security on your NBG420N, your network is accessible to any wireless networking device that is within range. If you choose this option, skip directly to Section 4.4 on page 54. Choose **Basic (WEP)** security if you want to configure WEP Encryption parameters. If you choose this option, go directly to Section 4.3.1 on page 53. This option is only available if WPS is not enabled. Choose **Extend** (**WPA-PSK** or **WPA2-PSK**) security to configure a Pre-Shared Key. Choose this option only if your wireless clients support WPA-PSK or WPA2-PSK respectively. If you choose this option, skip directly to Section 4.3.2 on page 54.
Channel Selection	The range of radio frequencies used by IEEE 802.11b/g/n wireless devices is called a channel. The device will automatically select the channel with the least interference.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

The wireless stations and NBG420N must use the same SSID, channel ID and WEP encryption key (if WEP is enabled), WPA-PSK (if WPA-PSK is enabled) or WPA2-PSK (if WPA2-PSK is enabled) for wireless communication.

4.3.1 Basic (WEP) Security

Choose **Basic (WEP)** to setup WEP Encryption parameters.

Figure 18 Wizard Step 2: Basic (WEP) Security


STEP 1 STEP 2 STEP 3 STEP 4
WIRELESS LAN
Passphrase
Use Passphrase to automatically generates a WEP key.
Passphrase
Generate
WEP Key
The higher the WEP Encryption, the higher the security but the slower the throughput.
Select 64-bit WEP, 128-bit WEP or 256-bit WEP to enable data encryption and select one of the Key radio buttons to use as the WEP key.
Entering a manual key in a Key field and selecting ASCII or Hex WEP key input method.
WEP Encryption
64-bit WEP
64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key(1-4).
(Select one WEP key as an active key to encrypt wireless data transmission.)
ASCII
Hex
Key 1
Key 2
Key 3
Key 4
<Back
Next >
Exit

The following table describes the labels in this screen.

Table 12 Wizard Step 2: Basic (WEP) Security

LABEL	DESCRIPTION
Passphrase	Type a Passphrase (up to 32 printable characters) and click **Generate**. The NBG420N automatically generates a WEP key.
WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to allow data encryption.
ASCII	Select this option in order to enter ASCII characters as the WEP keys.
HEX	Select this option to enter hexadecimal characters as the WEP keys. The preceding “0x” is entered automatically.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the NBG420N and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Back	Click **Back** to display the previous screen.

Table 12 Wizard Step 2: Basic (WEP) Security

LABEL	DESCRIPTION
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

4.3.2 Extend (WPA-PSK or WPA2-PSK) Security

Choose **Extend (WPA-PSK)** or **Extend (WPA2-PSK)** security in the Wireless LAN setup screen to set up a **Pre-Shared Key**.

Figure 19 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security

STEP 1 STEP 2 STEP 3 STEP 4
WIRELESS LAN
WPA2 Pre-Shared Key Setup
"WPA2-PSK" uses a "Pre-Shared Key" to authenticate wireless users and make sure they are allowed to access your network. Think of this pre-shared key as a shared password that you must know to get on the network.The pre-shared key should be at least 8 characters in length and made up of both letters and numbers.This pre-shared key is recommended to be different from the password you use to access this router or use to log-in to your ISP.
Pre-Shared Key
qwerty1234
<Back
Next >
Exit

The following table describes the labels in this screen.

Table 13 Wizard Step 2: Extend (WPA-PSK or WPA2-PSK) Security

LABEL	DESCRIPTION
Pre-Shared Key	Type from 8 to 63 case-sensitive ASCII characters. You can set up the most secure wireless connection by configuring WPA in the wireless LAN screens. You need to configure an authentication server to do this.
Back	Click **Back** to display the previous screen.
Next	Click **Next** to proceed to the next screen.
Exit	Click **Exit** to close the wizard screen without saving.

4.4 Connection Wizard: STEP 3: Internet Configuration

The NBG420N offers three Internet connection types. They are **Ethernet**, **PPP over Ethernet** or **PPTP**. The wizard attempts to detect which WAN connection type you are using. If the wizard does not detect a connection type, you must select one from the drop-down list box. Check with your ISP to make sure you use the correct type.

This wizard screen varies according to the connection type that you select.

Figure 20 Wizard Step 3: ISP Parameters.

The following table describes the labels in this screen,

Table 14 Wizard Step 3: ISP Parameters

CONNECTION TYPE	DESCRIPTION
Ethernet	Select the **Ethernet** option when the WAN port is used as a regular Ethernet.
PPPoE	Select the **PPP over Ethernet** option for a dial-up connection. If your ISP gave you an IP address and/or subnet mask, then select **PPTP**.
PPTP	Select the **PPTP** option for a dial-up connection.

4.4.1 Ethernet Connection

Choose **Ethernet** when the WAN port is used as a regular Ethernet. Continue to Section 4.4.4 on page 58.

Figure 21 Wizard Step 3: Ethernet Connection

4.4.2 PPPoE Connection

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, RADIUS).

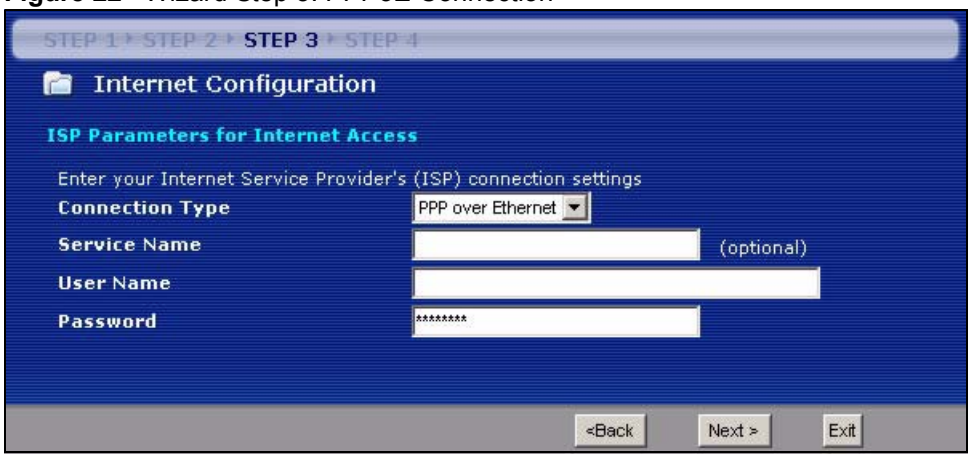
One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

By implementing PPPoE directly on the NBG420N (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG420N does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Refer to the appendix for more information on PPPoE.

Figure 22 Wizard Step 3: PPPoE Connection



The following table describes the labels in this screen.

Table 15 Wizard Step 3: PPPoE Connection

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Connection Type	Select the **PPP over Ethernet** option for a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

4.4.3 PPTP Connection

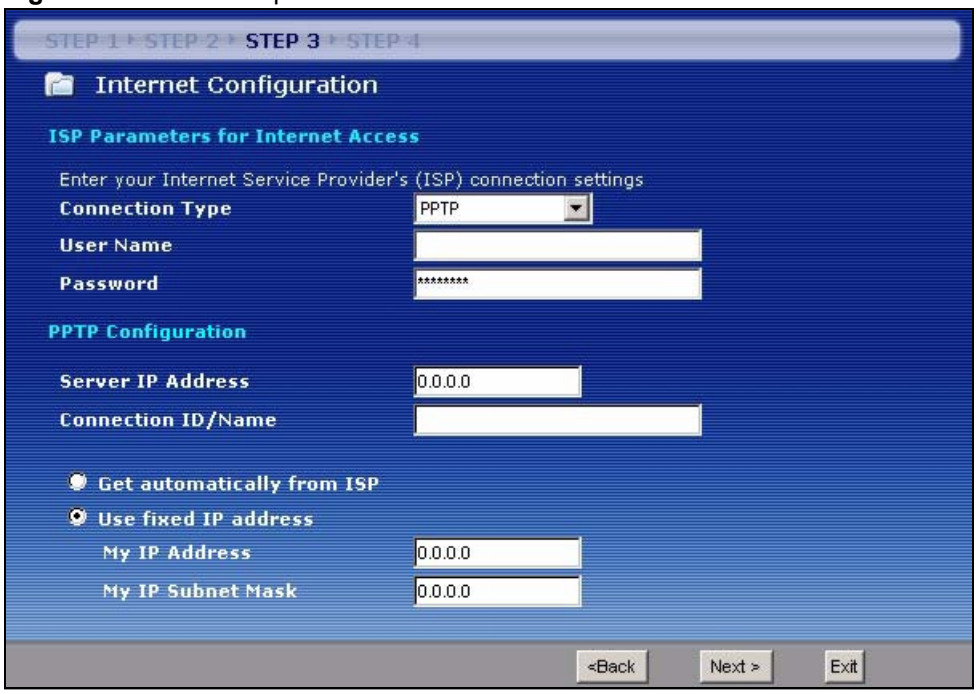
Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

Refer to the appendix for more information on PPTP.

The NBG420N supports one PPTP server connection at any given time.

Figure 23 Wizard Step 3: PPTP Connection



The following table describes the fields in this screen

Table 16 Wizard Step 3: PPTP Connection

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Connection Type	Select **PPTP** from the drop-down list box. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
PPTP Configuration	
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your ISP.
Get automatically from ISP	Select this radio button if your ISP did not assign you a fixed IP address.
Use fixed IP address	Select this radio button, provided by your ISP to give the NBG420N a fixed, unique IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Back	Click **Back** to return to the previous screen.

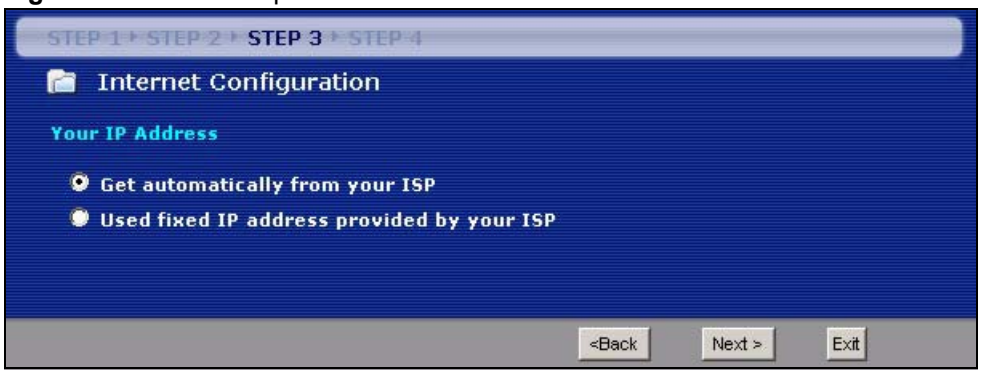
Table 16 Wizard Step 3: PPTP Connection

LABEL	DESCRIPTION
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

4.4.4 Your IP Address

The following wizard screen allows you to assign a fixed IP address or give the NBG420N an automatically assigned IP address depending on your ISP.

Figure 24 Wizard Step 3: Your IP Address



The following table describes the labels in this screen

Table 17 Wizard Step 3: Your IP Address

LABEL	DESCRIPTION
Get automatically from your ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection. If you choose this option, skip directly to Section 4.4.9 on page 61.
Use fixed IP address provided by your ISP	Select this option if you were given IP address and/or DNS server settings by the ISP. The fixed IP address should be in the same subnet as your broadband modem or router.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

4.4.5 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

Table 18 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

4.4.6 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your NBG420N, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your NBG420N will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the NBG420N unless you are instructed to do otherwise.

4.4.7 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The NBG420N can get the DNS server addresses in the following ways.

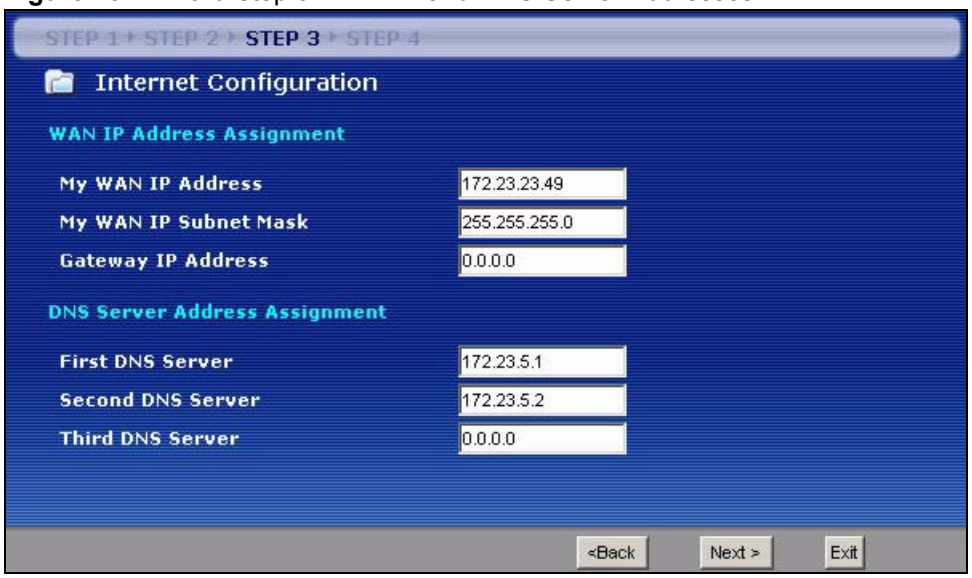
1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **Wizard** and/or **WAN > Internet Connection** screen.

2 If the ISP did not give you DNS server information, leave the **DNS Server** fields set to **0.0.0.0** in the **Wizard** screen and/or set to **From ISP** in the **WAN > Internet Connection** screen for the ISP to dynamically assign the DNS server IP addresses.

4.4.8 WAN IP and DNS Server Address Assignment

The following wizard screen allows you to assign a fixed WAN IP address and DNS server addresses.

Figure 25 Wizard Step 3: WAN IP and DNS Server Addresses



The following table describes the labels in this screen

Table 19 Wizard Step 3: WAN IP and DNS Server Addresses

LABEL	DESCRIPTION
WAN IP Address Assignment	
My WAN IP Address	Enter your WAN IP address in this field. The WAN IP address should be in the same subnet as your DSL/Cable modem or router.
My WAN IP Subnet Mask	Enter the IP subnet mask in this field.
Gateway IP Address	Enter the gateway IP address in this field.
System DNS Server Address Assignment (if applicable) DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The NBG420N uses a system DNS server (in the order you specify here) to resolve domain names for DDNS and the time server.	
First DNS Server Second DNS Server Third DNS Server	Enter the DNS server's IP address in the fields provided. If you do not configure a system DNS server, you must use IP addresses when configuring DDNS and the time server.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

4.4.9 WAN MAC Address

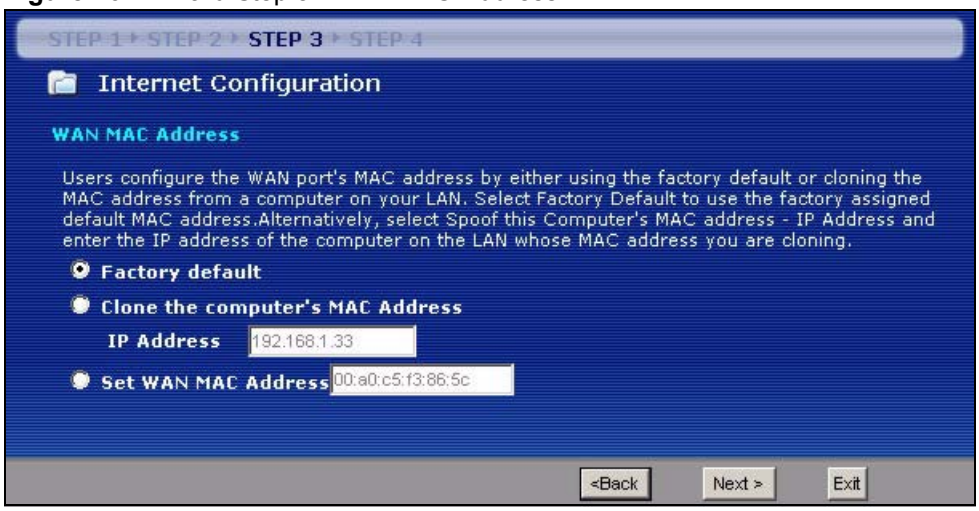
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Table 20 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(NBG420N LAN IP)

This screen allows users to configure the WAN port's MAC address by either using the NBG420N's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.

Figure 26 Wizard Step 3: WAN MAC Address


STEP 1 STEP 2 STEP 3 STEP 4
Internet Configuration
WAN MAC Address
Users configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Select Factory Default to use the factory assigned default MAC address.Alternatively, select Spoof this Computer's MAC address - IP Address and enter the IP address of the computer on the LAN whose MAC address you are cloning.
Factory default
Clone the computer's MAC Address
IP Address
192.168.1.33
Set WAN MAC Address
00:a0:c5:f3:86:5c
<Back
Next >
Exit

The following table describes the fields in this screen.

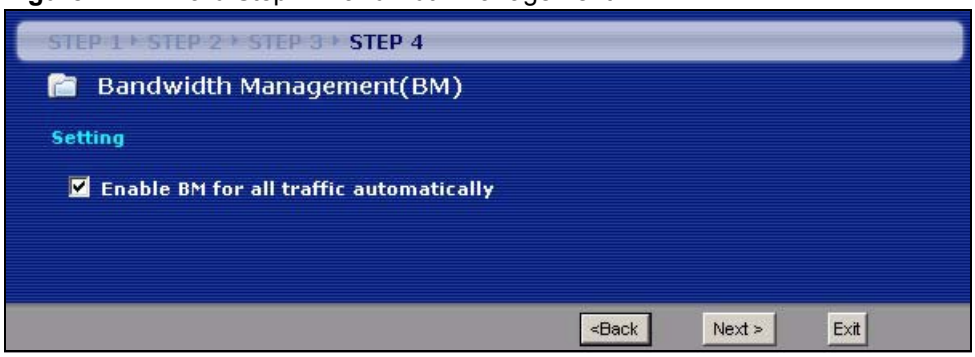
Table 21 Wizard Step 3: WAN MAC Address

LABEL	DESCRIPTION
Factory Default	Select **Factory Default** to use the factory assigned default MAC address.
Clone the computer's MAC address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

4.5 Connection Wizard: STEP 4: Bandwidth management

Bandwidth management allows you to control the amount of bandwidth going out through the NBG420N's WAN, LAN or WLAN port and prioritize the distribution of the bandwidth according to the traffic type. This helps keep one service from using all of the available bandwidth and shutting out other users.

Figure 27 Wizard Step 4: Bandwidth Management



The following fields describe the label in this screen.

Table 22 Wizard Step 4: Bandwidth Management

LABEL	DESCRIPTION
Enable BM for all traffic automatically	Select the check box to have the NBG420N apply bandwidth management to traffic going out through the NBG420N's WAN, LAN, HomePlug AV or WLAN port. Bandwidth is allocated according to the traffic type automatically. Real-time packets, such as VoIP traffic always get higher priority.
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.
Exit	Click **Exit** to close the wizard screen without saving.

4.6 Connection Wizard Complete

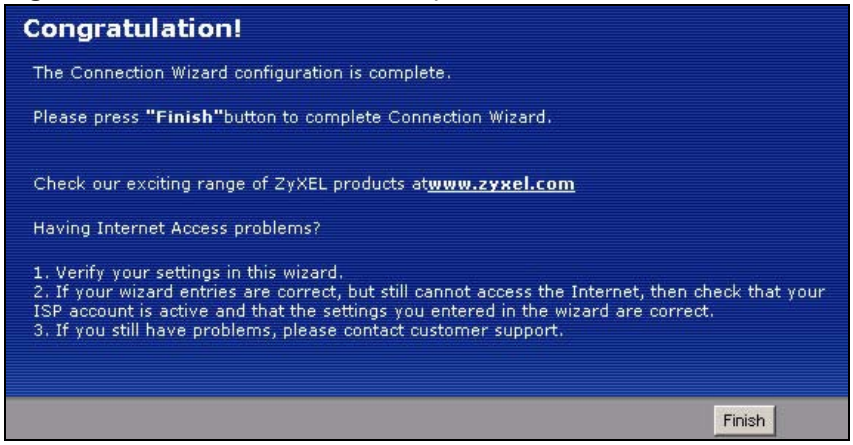
Click **Apply** to save your configuration.

Figure 28 Connection Wizard Save

STEP 1 STEP 2 STEP 3 STEP 4
Internet Configuration
Please Click the "Apply" Button to Complete the Connection Wizard.
Note:
If you are currently using a Wireless PC card to access this router AND you made changes to the SSID, then you will need to make the same changes to your Wireless PC card AFTER you click the Finish Button.
Once the changes have been made to the Wireless PC card, you will be able to connect back to the router and continue the configuration process.
<Back
Apply
Exit

Follow the on-screen instructions and click **Finish** to complete the wizard setup.

Figure 29 Connection Wizard Complete


Congratulation!
The Connection Wizard configuration is complete.
Please press "Finish"button to complete Connection Wizard.
Check our exciting range of ZyXEL products atwww.zyxel.com
Having Internet Access problems?
1. Verify your settings in this wizard.
2. If your wizard entries are correct, but still cannot access the Internet, then check that your ISP account is active and that the settings you entered in the wizard are correct.
3. If you still have problems, please contact customer support.
Finish

Well done! You have successfully set up your NBG420N to operate on your network and access the Internet.

5

AP Mode

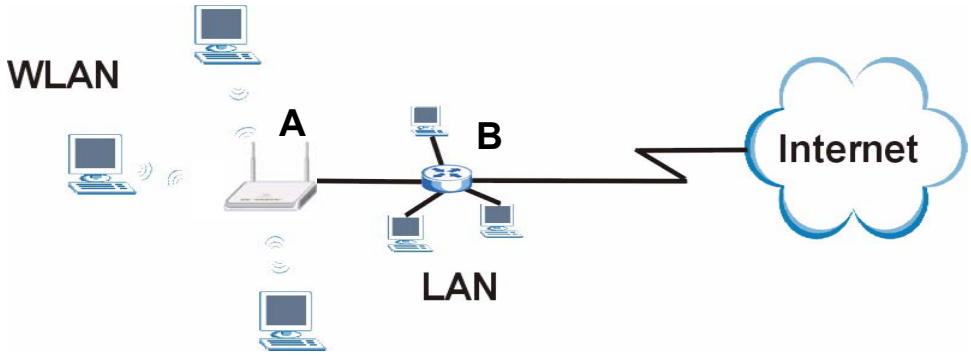
This chapter discusses how to configure settings while your NBG420N is set to **AP Mode**. Many screens that are available in **Router Mode** are not available in **AP Mode**.

See Chapter 6 on page 73 for an example of setting up a wireless network in AP mode.

5.1 AP Mode Overview

Use your NBG420N as an AP if you already have a router or gateway on your network. In this mode your device bridges a wired network (LAN) and wireless LAN (WLAN) in the same subnet. See the figure below for an example.

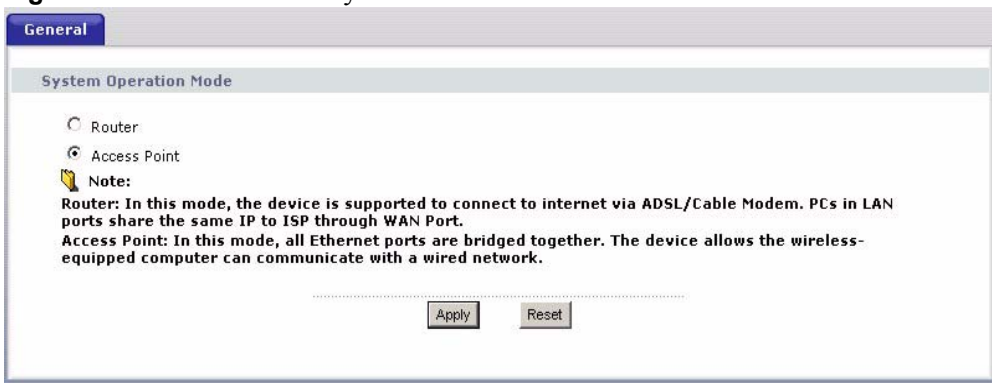
Figure 30 Wireless Internet Access in AP Mode



5.2 Setting your NBG420N to AP Mode

1. Log into the web configurator if you haven't already. See the Quick start Guide for instructions on how to do this.
2. To set your NBG420N to **AP Mode**, go to **Maintenance > Sys OP Mode > General** and select **Access Point.**

Figure 31 Maintenance > Sys OP Mode > General


General
System Operation Mode
Router
Access Point
Note:
Router: In this mode, the device is supported to connect to internet via ADSL/Cable Modem. PCs in LAN ports share the same IP to ISP through WAN Port.
Access Point: In this mode, all Ethernet ports are bridged together. The device allows the wireless-equipped computer can communicate with a wired network.
Apply
Reset

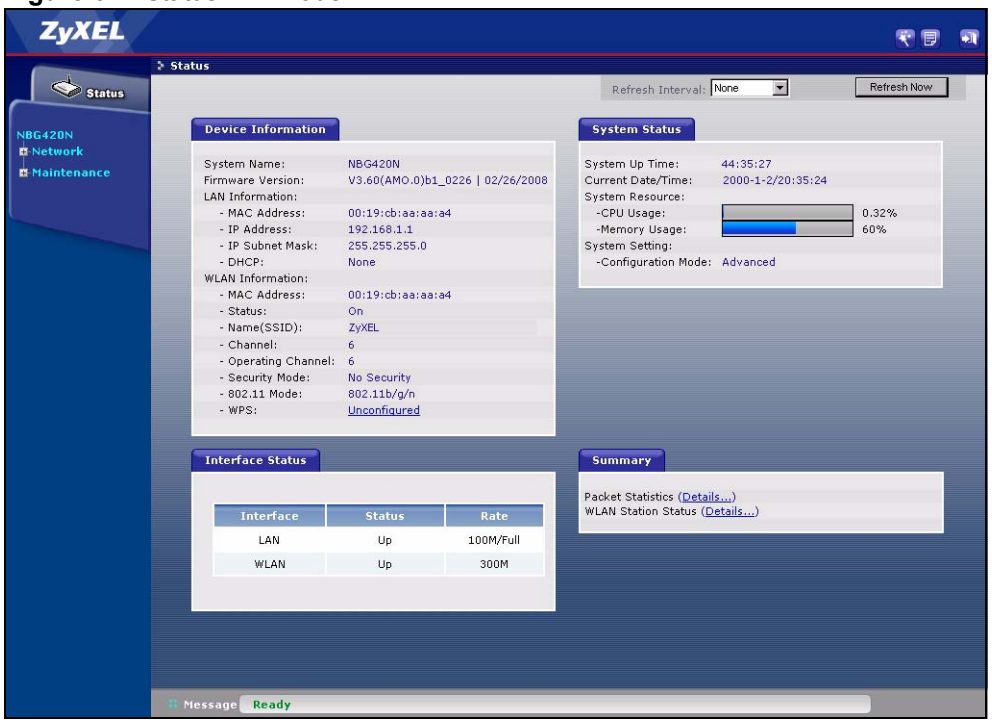
3 A pop-up appears providing information on this mode. Click **OK** in the pop-up message window. (See Section 24.2 on page 260 for more information on the pop-up.) Click **Apply**. Your NBG420N is now in **AP Mode**.

You do not have to log in again or restart your device when you change modes.

5.3 The Status Screen in AP Mode

Click on **Status**. The screen below shows the status screen in **AP Mode**.

Figure 32 Status: AP Mode



The following table describes the labels shown in the **Status** screen.

Table 23 Web Configurator Status Screen

LABEL	DESCRIPTION
Device Information	
System Name	This is the **System Name** you enter in the **Maintenance** > **System** > **General** screen. It is for identification purposes.
Firmware Version	This is the firmware version and the date created.
LAN Information	
- MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
- IP Address	This shows the LAN port's IP address.
- IP Subnet Mask	This shows the LAN port's subnet mask.
- DHCP	This shows the LAN port's DHCP role - **Client** or **None**.
WLAN Information	
- MAC Address	This shows the wireless adapter MAC Address of your device.
- Status	This shows the current status of the Wireless LAN - **On**, **Off or Off by scheduler**.
- Name (SSID)	This shows a descriptive name used to identify the NBG420N in the wireless LAN.
- Channel	This shows the channel number which you select manually.
- Operating Channel	This shows the channel number which the NBG420N is currently using over the wireless LAN.
- Security Mode	This shows the level of wireless security the NBG420N is using.
- 802.11 Mode	This shows the IEEE 802.11 standard that the NBG420N supports. Wireless clients must support the same standard in order to be able to connect to the NBG420N
- WPS	This shows the WPS (WiFi Protected Setup) Status. Click the status to display **Network** > **Wireless LAN** > **WPS** screen.
System Status	
System Uptime	This is the total time the NBG420N has been on.
Current Date/Time	This field displays your NBG420N's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the NBG420N's processing ability is currently used. When this percentage is close to 100%, the NBG420N is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management).
- Memory Usage	This shows what percentage of the heap memory the NBG420N is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT and the firewall.
System Setting	
- Configuration Mode	This shows whether the advanced screens of each feature are turned on (**Advanced**) or not (**Basic**).
Interface Status	
Interface	This displays the NBG420N port types. The port types are: **LAN** and **WLAN**.
Status	For the LAN port, this field displays **Down** (line is down) or **Up** (line is up or connected). For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.

Table 23 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
Rate	For the LAN ports, this displays the port speed and duplex setting or **N/A** when the line is disconnected. For the WLAN, it displays the maximum transmission rate when the WLAN is enabled and **N/A** when the WLAN is disabled.
Summary	
Packet Statistics	Use this screen to view port status and packet specific statistics.
WLAN Station Status	Use this screen to view the wireless stations that are currently associated to the NBG420N.

5.3.1 Navigation Panel

Use the menu in the navigation panel to configure NBG420N features in **AP Mode**.

The following screen and table show the features you can configure in **AP Mode**.

Figure 33 Menu: AP Mode

The following table describes the sub-menus.

Table 24 Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the NBG420N's general device, system and interface status information. Use this screen to access the wizard, and summary statistics tables.
Network		

Table 24 Screens Summary

LINK	TAB	FUNCTION
Wireless LAN	General	Use this screen to configure wireless LAN.
	MAC Filter	Use the MAC filter screen to configure the NBG420N to block access to devices or block the devices from accessing the NBG420N.
	Advanced	This screen allows you to configure advanced wireless settings.
	QoS	Use this screen to configure Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS allows you to prioritize wireless traffic according to the delivery requirements of individual services.
	WPS	Use this screen to configure WPS.
	WPS Station	Use this screen to add a wireless station using WPS.
	Scheduling	Use this screen to schedule the times the Wireless LAN is enabled.
LAN	IP	Use this screen to configure LAN IP address and subnet mask or to get the LAN IP address from a DHCP server.
Maintenance		
System	General	Use this screen to view and change administrative settings such as system and domain names, password and inactivity timer.
	Time Setting	Use this screen to change your NBG420N's time and date.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your NBG420N's log settings.
Tools	Firmware	Use this screen to upload firmware to your NBG420N.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your NBG420N.
	Restart	This screen allows you to reboot the NBG420N without turning the power off.
	Wake On LAN	Use this screen to remotely turn on a device on the network.
Config Mode	General	This screen allows you to display or hide the advanced screens or features.
Sys OP Mode	General	This screen allows you to select whether your device acts as a Router or a Access Point.
Language		This screen allows you to select the language you prefer.

5.4 Configuring Your Settings

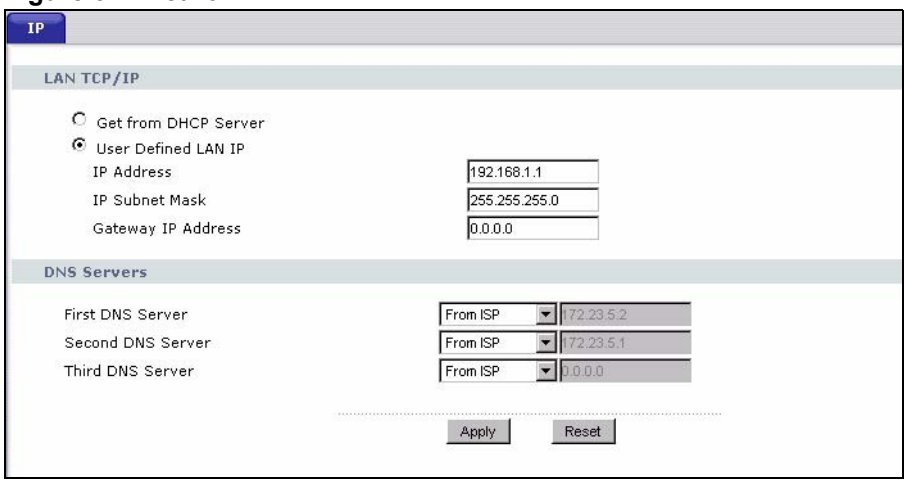
5.4.1 LAN Settings

Use this section to configure your LAN settings while in **AP Mode**.

Click **Network > LAN** to see the screen below.

If you change the IP address of the NBG420N in the screen below, you will need to log into the NBG420N again using the new IP address.

Figure 34 Network > LAN > IP



The table below describes the labels in the screen.

Table 25 Network > LAN > IP

LABEL	DESCRIPTION
Get from DHCP Server	Select this option to allow the NBG420N to obtain an IP address from a DHCP server on the network. You must connect the WAN port to a device with a DHCP server enabled (such as a router or gateway). Without a DHCP server the NBG420N will have no IP address. You need to find out the IP address the DHCP server assigns to the NBG420N and use that address to log in to the NBG420N again.
User Defined LAN IP	Select this option to set the NBG420N's IP address. This setting is selected by default. Check the IP address is on the same domain as other devices on your network.
IP Address	Type the IP address in dotted decimal notation. The default setting is 192.168.1.1. If you change the IP address you will have to log in again with the new IP address.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG420N will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the NBG420N.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your NBG420N that will forward the packet to the destination. In **AP Mode**, the gateway must be a router on the same segment as your NBG420N.
DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information. The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the NBG420N.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.4.2 WLAN and Maintenance Settings

The configuration of wireless and maintenance settings in **AP Mode** is the same as for **Router Mode**.

- See Chapter 5 on page 69 for information on the configuring your wireless network.
- See Maintenance and Troubleshooting (227) for information on the configuring your Maintenance settings.

5.5 Logging in to the Web Configurator in AP Mode

1. Connect your computer to the LAN port of the NBG420N.
2. The default IP address if the NBG420N is “192.168.1.1”. In this case, your computer must have an IP address in the range between “192.168.1.2” and “192.168.1.255”.
3. Click **Start > Run** on your computer in Windows.
4. Type “cmd” in the dialog box.
5. Type “ipconfig” to show your computer’s IP address. If your computer’s IP address is not in the correct range then see Appendix D on page 293 for information on changing your computer’s IP address.
6. After you’ve set your computer’s IP address, open a web browser such as Internet Explorer and type “192.168.1.1” as the web address in your web browser.

See Chapter 6 on page 73 for a tutorial on setting up a network with an AP.

6

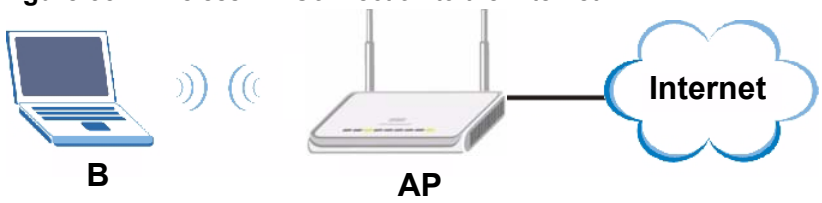
Tutorials

6.1 Wireless Tutorials

6.1.1 How to Connect to the Internet from an AP

This section gives you an example of how to set up an access point (**AP**) and wireless client (a notebook (**B**), in this example) for wireless communication. **B** can access the Internet through the AP wirelessly.

Figure 35 Wireless AP Connection to the Internet



6.1.2 Configure Wireless Security Using WPS on both your NBG420N and Wireless Client

This section gives you an example of how to set up wireless network using WPS. This example uses the NBG420N as the AP and NWD210N as the wireless client which connects to a notebook.

The wireless client must be a WPS-aware device (for example, a WPS USB adapter or PCI card).

There are two WPS methods for creating a secure connection. This tutorial shows you how to do both.

- **Push Button Configuration (PBC)** - create a secure wireless network simply by pressing a button. See Section 6.1.2.1 on page 74.This is the easier method.
- **PIN Configuration** - create a secure wireless network simply by entering a wireless client's PIN (Personal Identification Number) in the NBG420N's interface. See Section 6.1.2.2 on page 75. This is the more secure method, since one device can authenticate the other.

6.1.2.1 Push Button Configuration (PBC)

1. Make sure that your NBG420N is turned on and that it is within range of your computer.
2. Make sure that you have installed the wireless client (this example uses the NWD210N) driver and utility in your notebook.
3. In the wireless client utility, find the WPS settings. Enable WPS and press the WPS button (**Start** or **WPS** button)
4. Log into NBG420N's web configurator and press the **Push Button** button in the **Network** > **Wireless Client** > **WPS Station** screen.

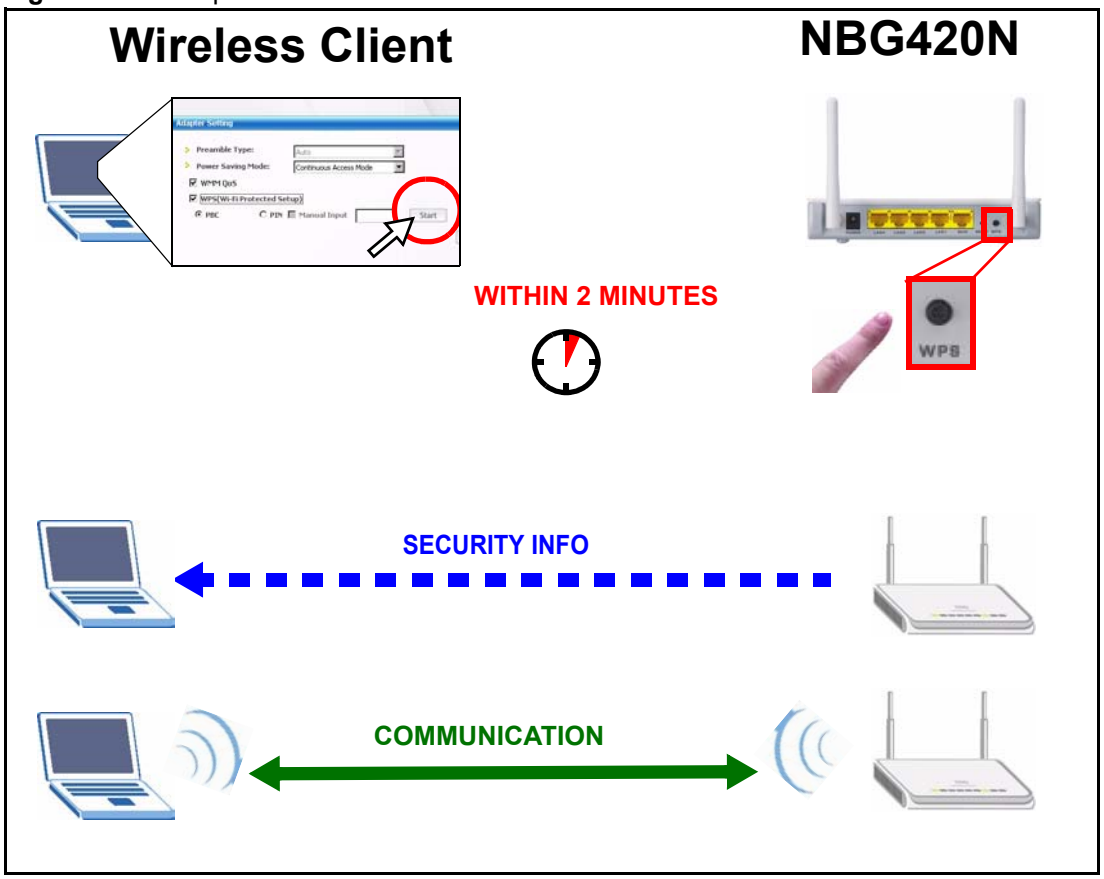
Your NBG420N has a WPS button located on its panel, as well as a WPS button in its configuration utility. Both buttons have exactly the same function; you can use one or the other.

It doesn't matter which button is pressed first. You must press the second button within two minutes of pressing the first one.

The NBG420N sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the NBG420N securely.

The following figure shows you an example to set up wireless network and security by pressing a button on both NBG420N and wireless client (the NWD210N in this example).

Figure 36 Example WPS Process: PBC Method



6.1.2.2 PIN Configuration

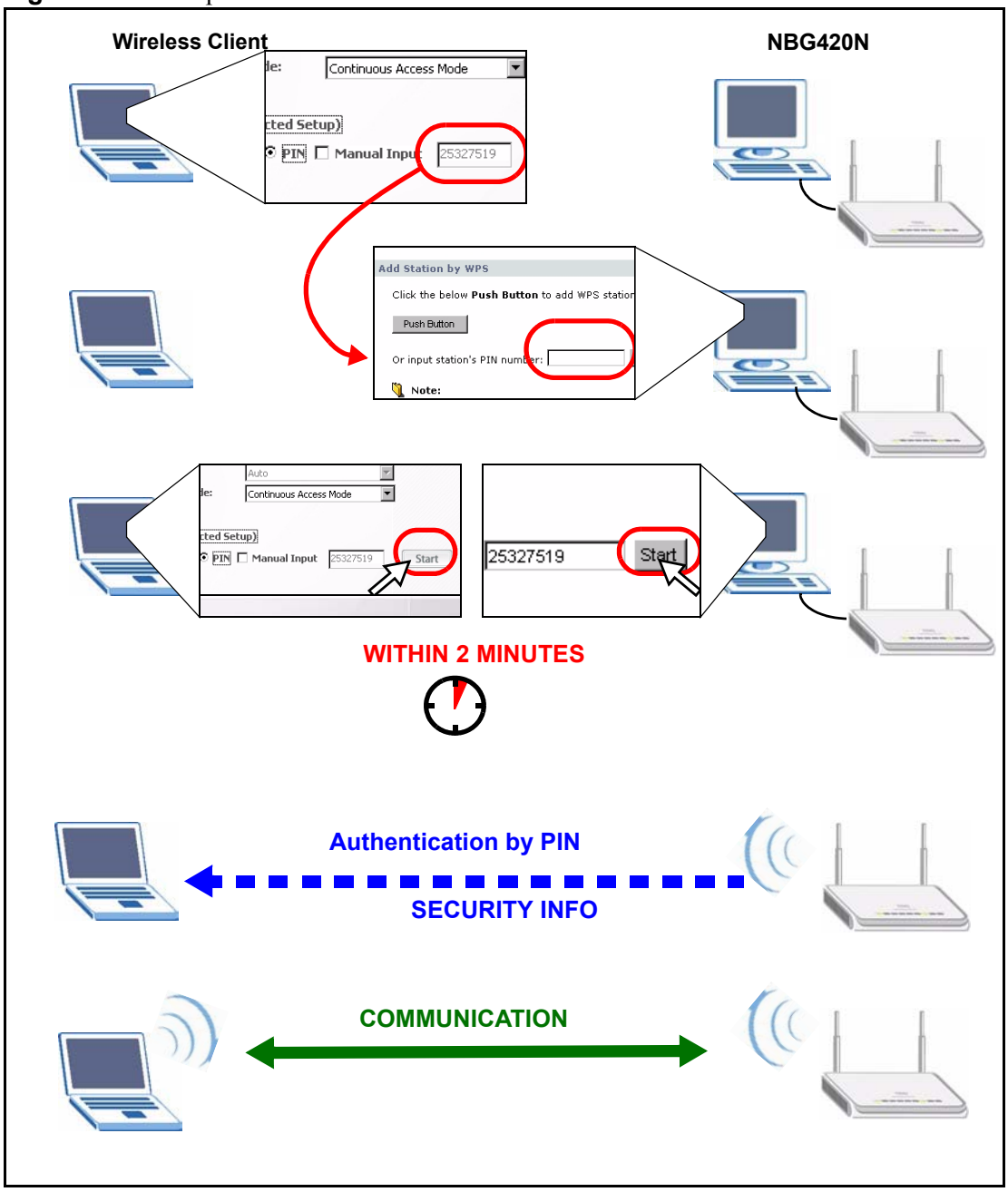
When you use the PIN configuration method, you need to use both NBG420N's configuration interface and the client's utilities.

1. Launch your wireless client's configuration utility. Go to the WPS settings and select the PIN method to get a PIN number.
2. Enter the PIN number to the **PIN** field in the **Network** > **Wireless LAN** > **WPS Station** screen on the NBG420N.
3. Click **Start** buttons (or button next to the PIN field) on both the wireless client utility screen and the NBG420N's **WPS Station** screen within two minutes.

The NBG420N authenticates the wireless client and sends the proper configuration settings to the wireless client. This may take up to two minutes. Then the wireless client is able to communicate with the NBG420N securely.

The following figure shows you the example to set up wireless network and security on NBG420N and wireless client (ex. NWD210N in this example) by using PIN method.

Figure 37 Example WPS Process: PIN Method



6.1.3 Enable and Configure Wireless Security without WPS on your NBG420N

This example shows you how to configure wireless security settings with the following parameters on your NBG420N.

SSID	SSID_Example3

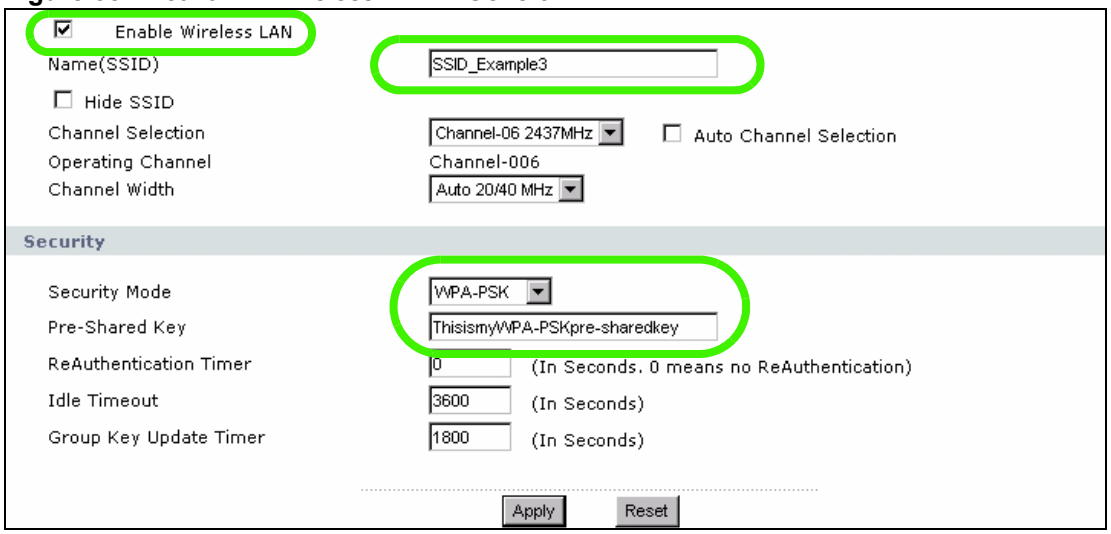
Channel	6
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

Follow the steps below to configure the wireless settings on your NBG420N.

The instructions require that your hardware is connected (see the Quick Start Guide) and you are logged into the web configurator through your LAN connection (see Section 3.2 on page 37).

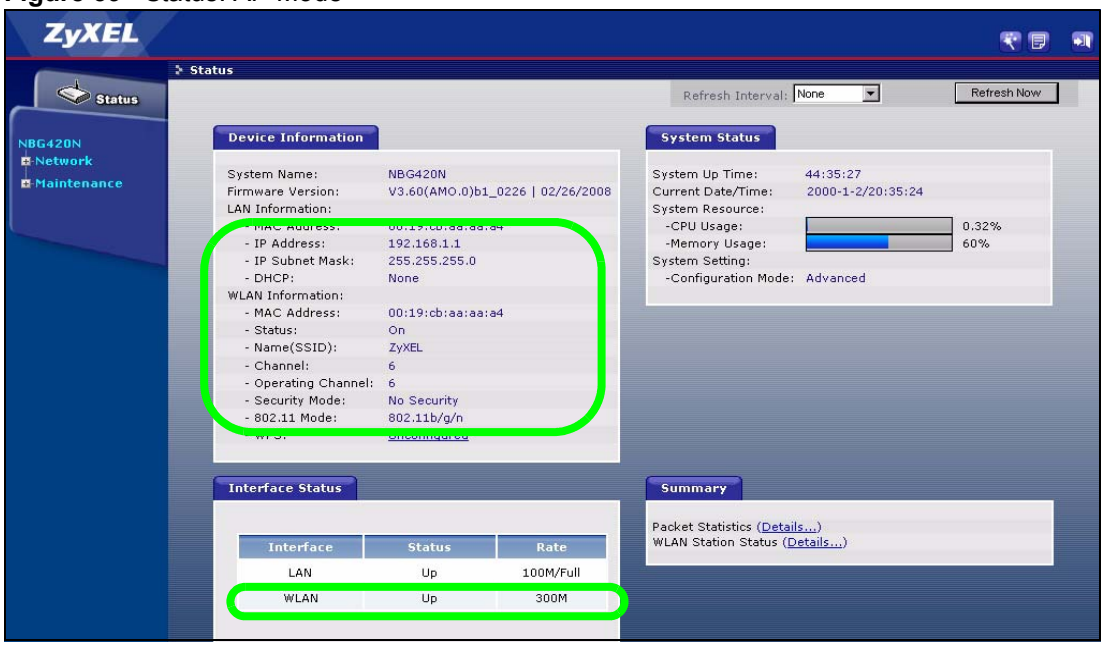
1. Open the **Wireless LAN > General** screen in the AP's web configurator.
2. Make sure the **Enable Wireless LAN** check box is selected.
3. Enter **SSID_Example3** as the SSID and select a channel.
4. Set security mode to **WPA-PSK** and enter **ThisismyWPA-PSKpre-sharedkey** in the **Pre-Shared Key** field. Click **Apply**.

Figure 38 Network > Wireless LAN > General



5. Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

Figure 39 Status: AP Mode

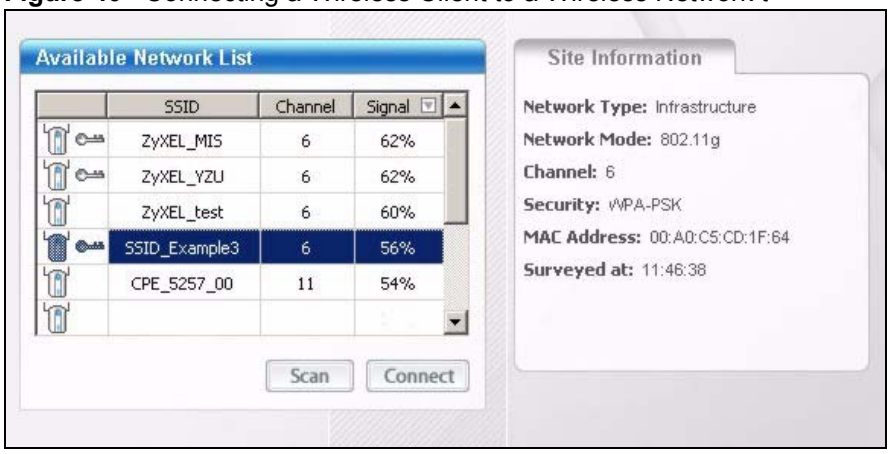


6.1.4 Configure Your Notebook

We use the ZyXEL M-302 wireless adapter utility screens as an example for the wireless client. The screens may vary for different models.

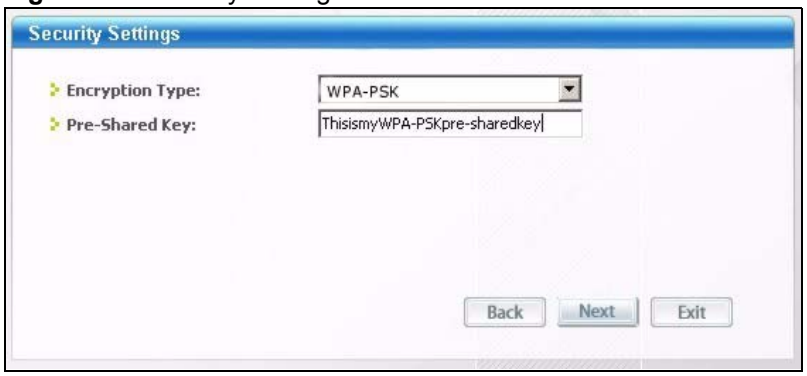
1. The NBG420N supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer's wireless adapter supports one of these standards.
2. Wireless adapters come with software sometimes called a "utility" that you install on your computer. See your wireless adapter's User's Guide for information on how to do that.
3. After you've installed the utility, open it. If you cannot see your utility's icon on your screen, go to **Start > Programs** and click on your utility in the list of programs that appears. The utility displays a list of APs within range, as shown in the example screen below.
4. Select SSID_Example3 and click **Connect**.

Figure 40 Connecting a Wireless Client to a Wireless Network t



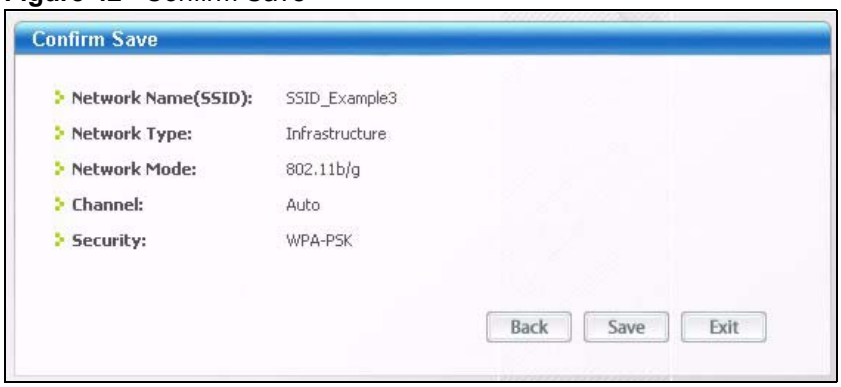
5 Select WPA-PSK and type the security key in the following screen. Click **Next**.

Figure 41 Security Settings



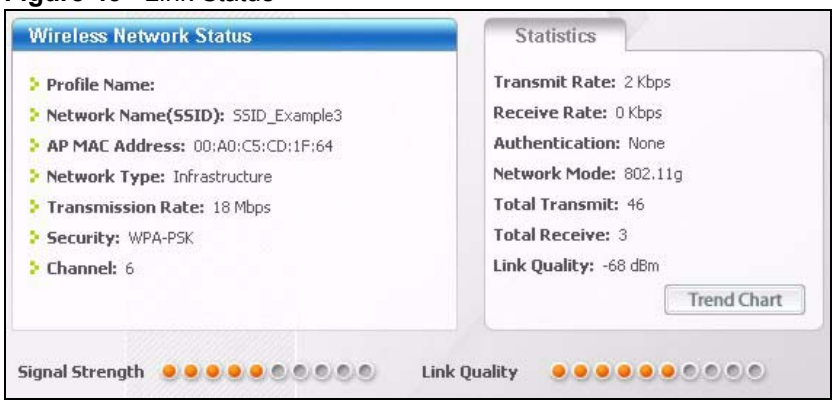
6 The **Confirm Save** window appears. Check your settings and click **Save** to continue.

Figure 42 Confirm Save



7 Check the status of your wireless connection in the screen below. If your wireless connection is weak or you have no connection, see the Troubleshooting section of this User's Guide.

Figure 43 Link Status

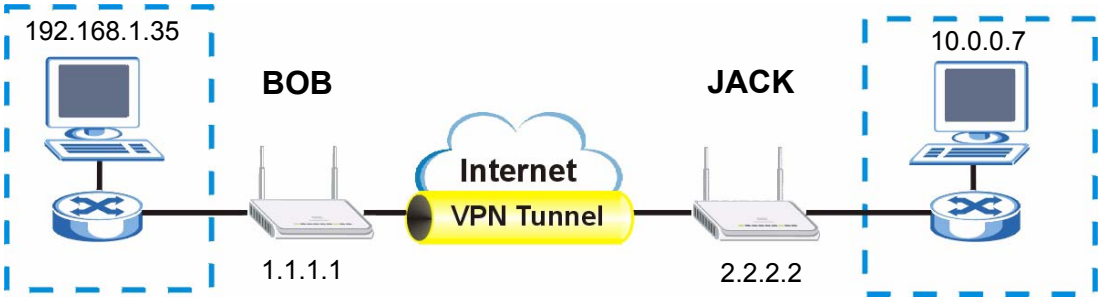


8 If your connection is successful, open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

6.2 Site-To-Site VPN Tunnel Tutorial

Bob and Jack want to setup a VPN connection between their offices. Bob and Jack each have a NBG420N router and a static WAN IP address. This tutorial covers how to configure their NBG420Ns to create a secure connection.

Figure 44 Site-To-Site VPN Tunnel



The following table describes the VPN settings that must be configured on Bob and Jack's NBG420N routers.

Table 26 Site-To-Site VPN Tunnel Settings

SETTING	BOB'S NBG420N	JACK'S NBG420N
Active	YES	YES
IPSec Keying Mode	IKE	IKE
Local Address	192.168.1.35	10.0.0.7
Local Address End /Mask	192.168.1.35	10.0.0.7
Remote Address	10.0.0.7	192.168.1.35
Remote Address End /Mask	10.0.0.7	192.168.1.35
My IP Address	1.1.1.1	2.2.2.2

Table 26 Site-To-Site VPN Tunnel Settings (continued)

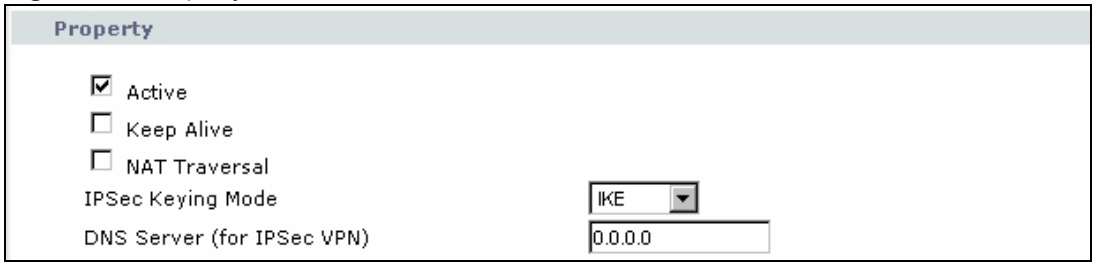
SETTING	BOB'S NBG420N	JACK'S NBG420N
Local ID Type	IP	IP
Local Content	1.1.1.1	2.2.2.2
Secure Gateway Address	2.2.2.2	1.1.1.1
Peer ID Type	IP	IP
Peer Content	2.2.2.2	1.1.1.1
Encapsulation Mode	Tunnel	Tunnel
IPSec Protocol	ESP	ESP
Pre-Shared Key	ThisIsMySecretKey	ThisIsMySecretKey
Encryption Algorithm	3DES	3DES
Authentication Algorithm	SHA1	SHA1

6.2.1 Configuring Bob's NBG420N VPN Settings

To configure these settings Bob uses the NBG420N web configurator.

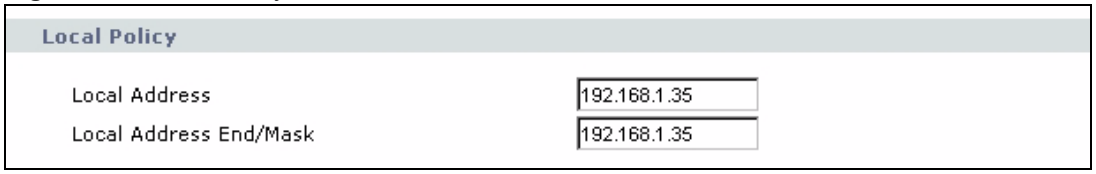
1. Log into the NBG420N web configurator and click **VPN** > **Modify** icon. This displays the **VPN Rule Setup** (basic) screen.
2. Select the **Active** checkbox to enable the VPN rule after it has been created. Make sure IKE is selected as the **IPSec Keying Mode**.

Figure 45 Property



3. Enter the IP address "192.168.1.35" in the **Local Address** text box. This is the IP address of Bob's computer. Enter the IP address "192.168.1.35" in the **Local Address End/Mask** text box. This value is the same as Bob only wants Jack to access this single IP address.

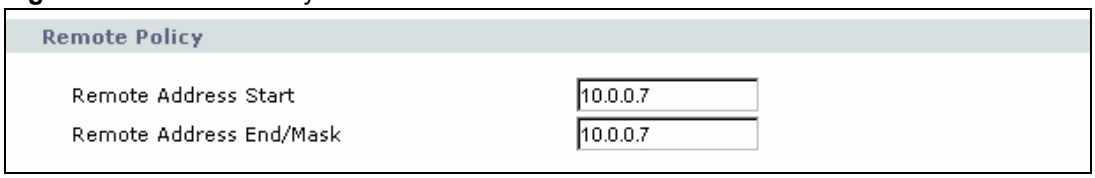
Figure 46 Local Policy



4. Enter the IP address "10.0.0.7" in the **Remote Address Start** text box. This is the IP address of Jack's computer. Enter the IP address "10.0.0.7" in the **Remote Address**

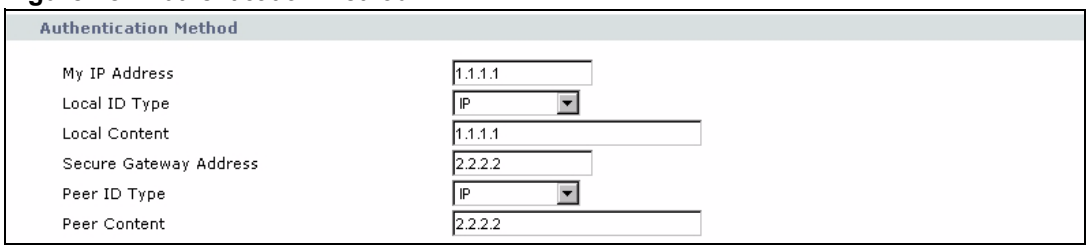
End/Mask text box. This value is the same as Jack only wants Bob to access this single IP address.

Figure 47 Remote Policy



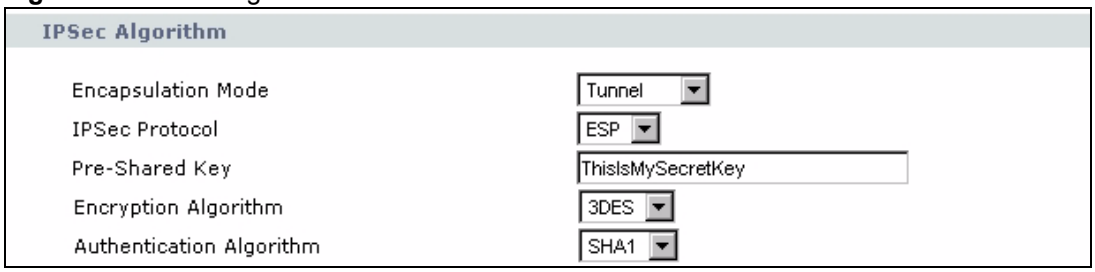
5. Enter the IP address "1.1.1.1" in the **My IP Address** text box. This is Bob's WAN IP address.
6. Select IP as the **Local ID Type**. This is the type of content that will be used to identify Bob's NBG420N. Enter the IP address "1.1.1.1" in the **Local Content** text box. This identifies Bob's NBG420N to Jack's NBG420N.
7. Enter the IP address "2.2.2.2" in the **Secure Gateway Address** text box. This is Jack's WAN IP address.
8. Select IP as the **Peer ID Type**. This is Jack's **Local ID Type**. Enter "2.2.2.2" in the **Peer Content** text box. This is Jack's **Local Content** WAN IP address.

Figure 48 Authentication Method



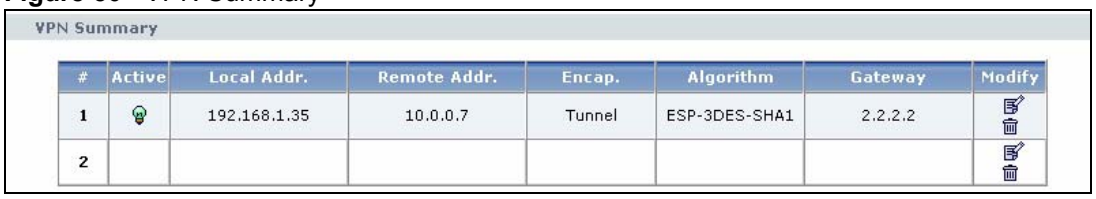
9. Select **Tunnel** as the **Encapsulation Mode** and **ESP** as the **IPSec Protocol**.
10. Enter "ThisIsMySecretKey" as the **Pre-Shared Key**. This is the password for the VPN tunnel that only Bob and Jack know.
11. Select **3DES** as the encyption algorithm. Select the authentication algorithm as **SHA1**. These algorithms are more secure.

Figure 49 IPSec Algorithm



12. Click **Apply** to save the new rule and click **VPN** to return to the **VPN Summary** screen. The new VPN rule is displayed as shown below.

Figure 50 VPN Summary

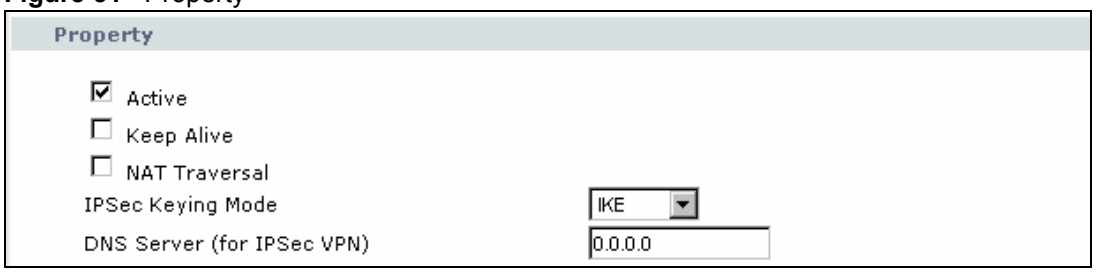


6.2.2 Configuring Jack's NBG420N VPN Settings

To configure these settings Jack uses the NBG420N web configurator.

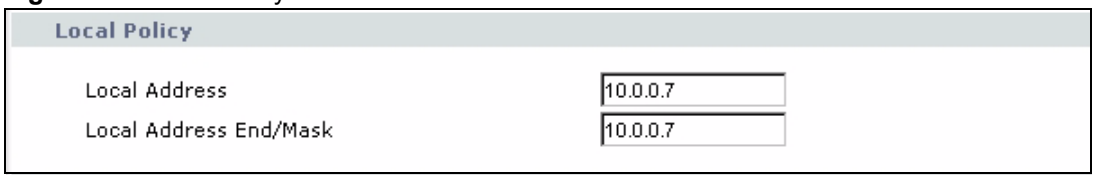
1. Log into the NBG420N web configurator and click **VPN** > **Modify** icon. This displays the **VPN Rule Setup** (basic) screen.
2. Select the **Active** checkbox to enable the VPN rule after it has been created. Make sure IKE is selected as the **IPSec Keying Mode**.

Figure 51 Property



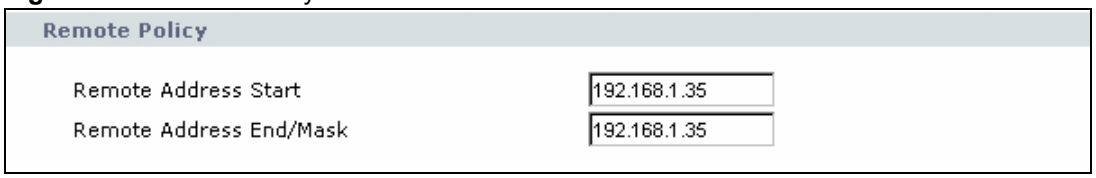
3. Enter the IP address "10.0.0.7" in the **Local Address** text box. This is the IP address of Jack's computer. Enter the IP address "10.0.0.7" in the **Local Address End/Mask** text box. This value is the same as Jack only wants Bob to access this single IP address.

Figure 52 Local Policy



4. Enter the IP address "192.168.1.35" in the **Remote Address Start** text box. This is the IP address of Jack's computer. Enter the IP address "192.168.1.35" in the **Remote Address End/Mask** text box. This value is the same as Bob only wants Jack to access this single IP address.

Figure 53 Remote Policy



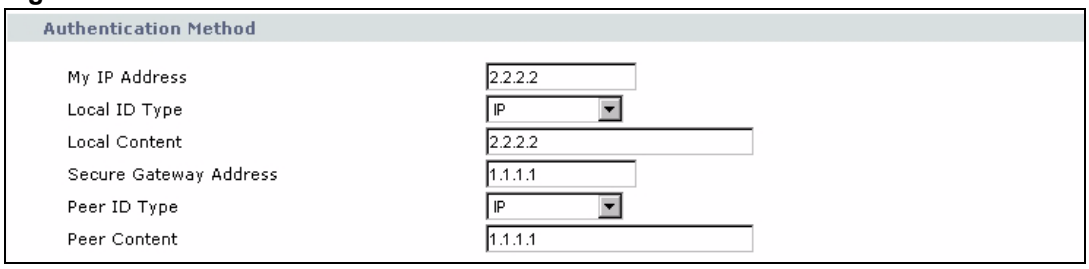
5. Enter the IP address "2.2.2.2" in the **My IP Address** text box. This is Jack's WAN IP address.

6 Select IP as the **Local ID Type**. This is the type of content that will be used to identify Jack's NBG420N. Enter the IP address "2.2.2.2" in the **Local Content** text box. This identifies Jack's NBG420N to Bob's NBG420N.

7 Enter the IP address "1.1.1.1" in the **Secure Gateway Address** text box. This is Bob's WAN IP address.

8 Select IP as the **Peer ID Type**. This is Bob's **Local ID Type**. Enter "1.1.1.1" in the **Peer Content** text box. This is Bob's **Local Content** WAN IP address.

Figure 54 Authentication Method

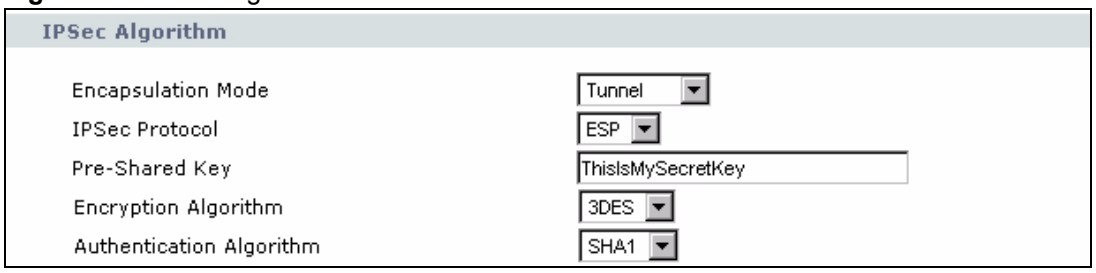


9 Select **Tunnel** as the **Encapsulation Mode** and **ESP** as the **IPSec Protocol**.

10 Enter "ThisIsMySecretKey" as the **Pre-Shared Key**. This is the password for the VPN tunnel that only Bob and Jack know.

11 Select **3DES** as the encyption algorithm. Select the authentication algorithm as **SHA1**. These algorithms are more secure.

Figure 55 IPSec Algorithm



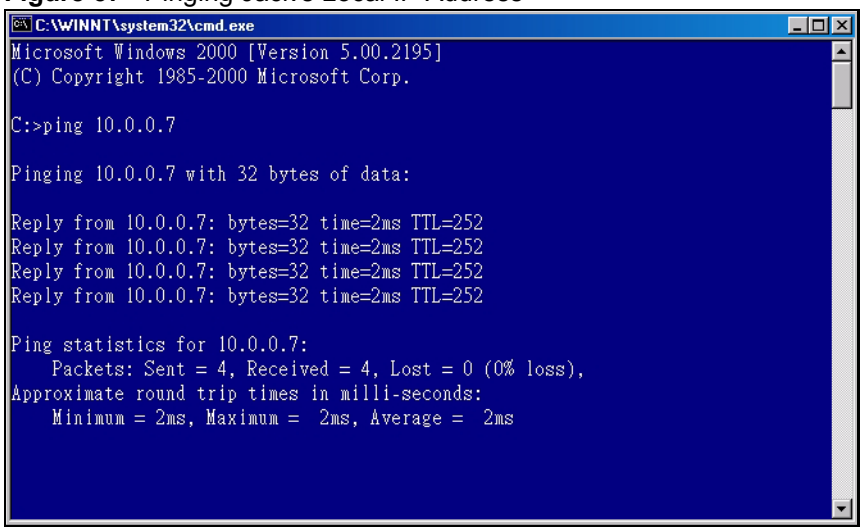
12 Click **Apply** to save the new rule and click **VPN** in the web configurator menu to return to the **VPN Summary** screen. The new VPN rule is displayed as shown below.

Figure 56 VPN Summary

6.2.3 Checking the VPN Connection

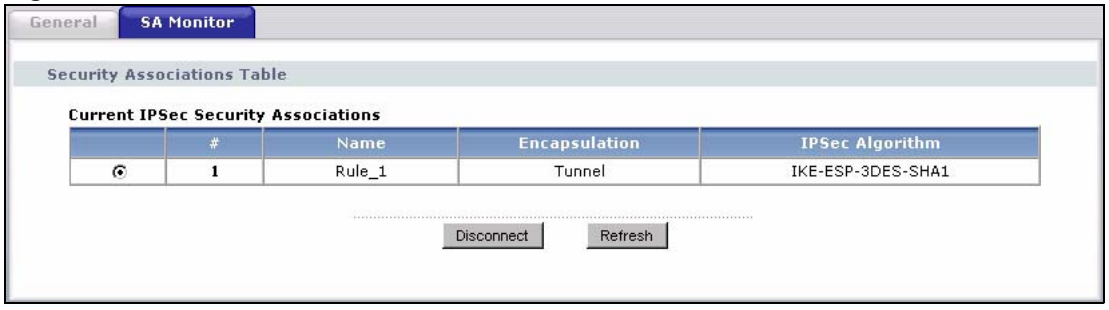
Check if the VPN connection is working by pinging the computer on the other side of the VPN connection. In the example below Bob is pinging Jack's computer.

Figure 57 Pinging Jack's Local IP Address


C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:>ping 10.0.0.7
Pinging 10.0.0.7 with 32 bytes of data:
Reply from 10.0.0.7: bytes=32 time=2ms TTL=252
Reply from 10.0.0.7: bytes=32 time=2ms TTL=252
Reply from 10.0.0.7: bytes=32 time=2ms TTL=252
Reply from 10.0.0.7: bytes=32 time=2ms TTL=252
Ping statistics for 10.0.0.7:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 2ms, Average = 2ms

Pinging is successful which means a VPN tunnel has been established between Bob and Jack's NBG420Ns. Congratulations! To check this VPN connection click **VPN** > **SA Monitor** in the web configurator.

Figure 58 SA Monitor



If pinging is not successful check the VPN settings on both devices and try again. If you are still having problems make sure the VPN settings in the Advanced options are also the same.

For more information on VPN including field descriptions refer to Chapter 15 on page 165.

PART II
Network

Wireless LAN (89)
WAN (117)
LAN (127)
DHCP (133)
Network Address Translation (NAT) (137)
Dynamic DNS (147)

7

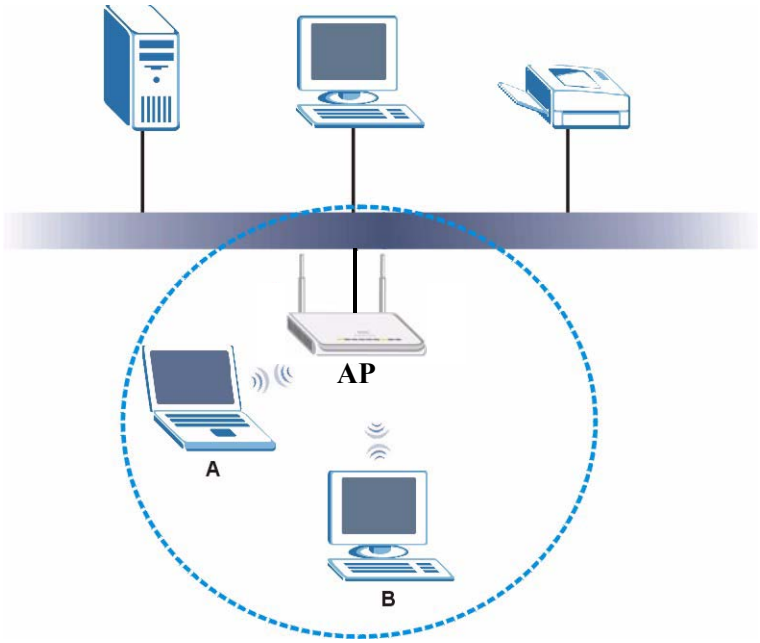
Wireless LAN

This chapter discusses how to configure the wireless network settings in your NBG420N. See the appendices for more detailed information about wireless networks.

7.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 59 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices A and B are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your NBG420N is the AP.

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.
  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.
  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every wireless client in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

7.2 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

7.2.1 SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

7.2.2 MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

7.2.3 User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

If your AP does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

Local user databases also have an additional limitation that is explained in the next section.

7.2.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of user authentication. (See Section 7.2.3 on page 90 for information about this.)

Table 27 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
↕	Static WEP	
↕	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

When you select **WPA2** or **WPA2-PSK** in your NBG420N, you can also select an option (**WPA Compatible**) to support WPA as well. In this case, if some wireless clients support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA Compatible** option in the NBG420N.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

7.3 Roaming

A wireless station is a device with an IEEE 802.11a/b/g/n compliant wireless interface. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area.

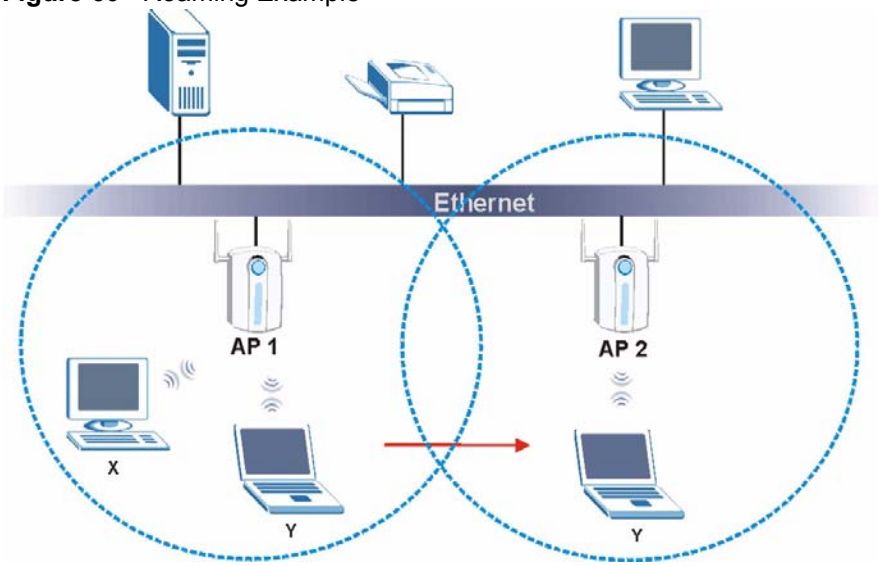
In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is known as roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the other access points on the LAN about the change. An example is shown in Figure 60 on page 93.

With roaming, a wireless LAN mobile user enjoys a continuous connection to the wired network through an access point while moving around the wireless LAN.

Enable roaming to exchange the latest bridge information of all wireless stations between APs when a wireless station moves between coverage areas. Wireless stations can still associate with other APs even if you disable roaming. Enabling roaming ensures correct traffic forwarding (bridge tables are updated) and maximum AP efficiency. The AP deletes records of wireless stations that associate with other APs (Non-ZyXEL APs may not be able to perform this). 802.1x authentication information is not exchanged (at the time of writing).

Figure 60 Roaming Example



The steps below describe the roaming process.

1. Wireless station **Y** moves from the coverage area of access point **AP 1** to that of access point **AP 2**.
2. Wireless station **Y** scans and detects the signal of access point **AP 2**.
3. Wireless station **Y** sends an association request to access point **AP 2**.
4. Access point **AP 2** acknowledges the presence of wireless station **Y** and relays this information to access point **AP 1** through the wired LAN.
5. Access point **AP 1** updates the new position of wireless station **Y**.

7.3.1 Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

1. All the access points must be on the same subnet and configured with the same ESSID.
2. If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
3. The adjacent access points should use different radio channels when their coverage areas overlap.
4. All access points must use the same port number to relay roaming information.
5. The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

7.4 Quality of Service

This section discusses the Quality of Service (QoS) features available on the NBG420N.

7.4.1 WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) ensures quality of service in wireless networks. It controls WLAN transmission priority on packets to be transmitted over the wireless network.

WMM QoS prioritizes wireless traffic according to delivery requirements. WMM QoS is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.

On APs without WMM QoS, all traffic streams are given the same access priority to the wireless network. If the introduction of another traffic stream creates a data transmission demand that exceeds the current network capacity, then the new traffic stream reduces the throughput of the other traffic streams.

The NBG420N uses WMM QoS to prioritize traffic streams according to the IEEE 802.1q tag or DSCP information in each packet's header. The NBG420N automatically determines the priority to use for an individual traffic stream. This prevents reductions in data transmission for applications that are sensitive to latency (delay) and jitter (variations in delay).

7.4.1.1 WMM QoS Priorities

The following table describes the WMM QoS priority levels that the NBG420N uses.

Table 28 WMM QoS Priorities

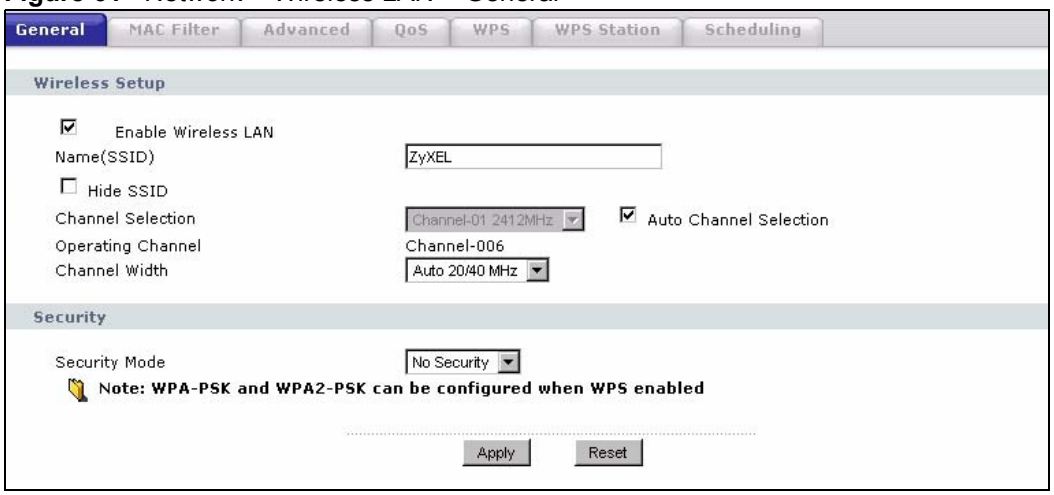
PRIORITY LEVEL	DESCRIPTION
voice (WMM_VOICE)	Typically used for traffic that is especially sensitive to jitter. Use this priority to reduce latency for improved voice quality.
video (WMM_VIDEO)	Typically used for traffic which has some tolerance for jitter but needs to be prioritized over other data traffic.
best effort (WMM_BEST_EFFORT)	Typically used for traffic from applications or devices that lack QoS capabilities. Use best effort priority for traffic that is less sensitive to latency, but is affected by long delays, such as Internet surfing.
background (WMM_BACKGROUND)	This is typically used for non-critical traffic such as bulk transfers and print jobs that are allowed but that should not affect other applications and users. Use background priority for applications that do not have strict latency and throughput requirements.

7.5 General Wireless LAN Screen

If you are configuring the NBG420N from a computer connected to the wireless LAN and you change the NBG420N's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the NBG420N's new settings.

Click **Network** > **Wireless LAN** to open the **General** screen.

Figure 61 Network > Wireless LAN > General



The following table describes the general wireless LAN labels in this screen.

Table 29 Network > Wireless LAN > General

LABEL	DESCRIPTION
Enable Wireless LAN	Click the check box to activate wireless LAN.
Name(SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Refer to the Connection Wizard chapter for more information on channels. This option is only available if **Auto Channel Selection** is disabled.
Auto Channel Selection	Select this check box for the NBG420N to automatically choose the channel with the least interference. Deselect this check box if you wish to manually select the channel using the **Channel Section** field.
Operating Channel	This displays the channel the NBG420N is currently using.
Channel Width	Select whether the NBG420N uses a wireless channel width of 20 or 40 MHz. A standard 20 MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. Because not all devices support 40 MHz channels, select **Auto 20/40MHz** to allow the NBG420N to adjust the channel bandwidth automatically.
Security Mode	Select **Static-WEP**, **WPA-PSK**, **WPA**, **WPA2-PSK**, or **WPA2** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See 7.5.2, 7.5.3, 7.5.4 sections. Or you can select **No Security** to allow any client to associate this network without authentication. Note: If you enable the WPS function, only **No Security**, **WPA-PSK** and **WPA2-PSK** are available in this field.

Table 29 Network > Wireless LAN > General

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to reload the previous configuration for this screen.

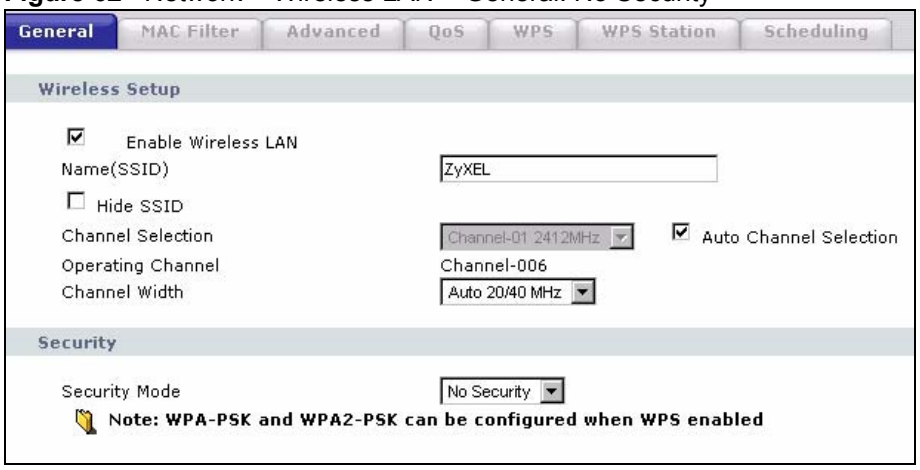
See the rest of this chapter for information on the other labels in this screen.

7.5.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption.

If you do not enable any wireless security on your NBG420N, your network is accessible to any wireless networking device that is within range.

Figure 62 Network > Wireless LAN > General: No Security



The following table describes the labels in this screen.

Table 30 Wireless No Security

LABEL	DESCRIPTION
Security Mode	Choose **No Security** from the drop-down list box.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to reload the previous configuration for this screen.

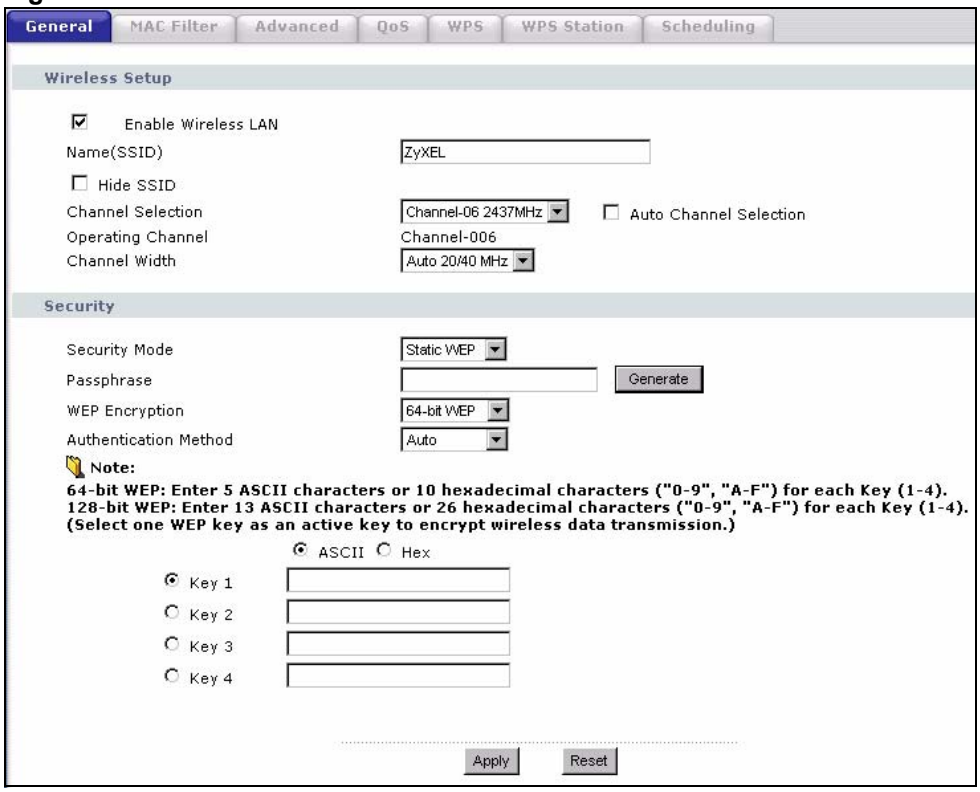
7.5.2 WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

Your NBG420N allows you to configure up to four 64-bit or 128-bit WEP keys but only one key can be enabled at any one time.

In order to configure and enable WEP encryption; click **Network** > **Wireless LAN** to display the **General** screen. Select **Static WEP** from the **Security Mode** list.

Figure 63 Network > Wireless LAN > General: Static WEP



The following table describes the wireless LAN security labels in this screen.

Table 31 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
Passphrase	Enter a passphrase (password phrase) of up to 32 printable characters and click **Generate**. The NBG420N automatically generates four different WEP keys and displays them in the **Key** fields below.
WEP Encryption	Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Authentication Method	This field is activated when you select **64-bit WEP** or **128-bit WEP** in the **WEP Encryption** field. Select **Auto** or **Shared Key** from the drop-down list box.
ASCII	Select this option in order to enter ASCII characters as WEP key.
Hex	Select this option in order to enter hexadecimal characters as a WEP key. The preceding "0x", that identifies a hexadecimal key, is entered automatically.

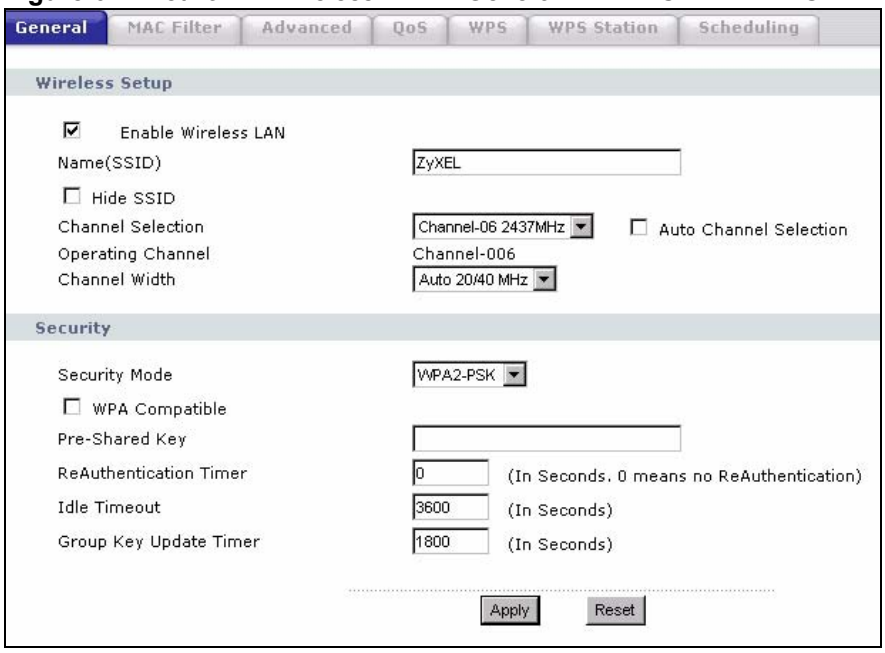
Table 31 Network > Wireless LAN > General: Static WEP

LABEL	DESCRIPTION
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the NBG420N and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one key, only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5.3 WPA-PSK/WPA2-PSK

Click **Network** > **Wireless LAN** to display the **General** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 64 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK



The following table describes the labels in this screen.

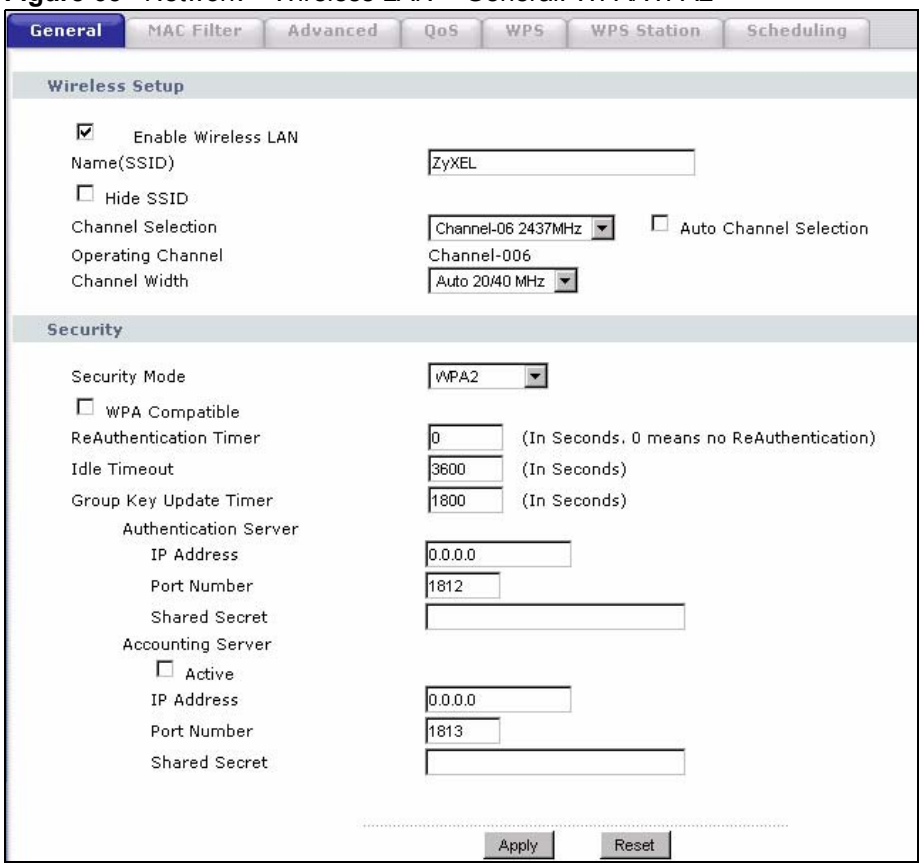
Table 32 Network > Wireless LAN > General: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Security Mode** field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the NBG420N even when the NBG420N is using WPA2-PSK or WPA2.
Pre-Shared Key	The encryption mechanisms used for **WPA/WPA2** and **WPA-PSK/WPA2-PSK** are the same. The only difference between the two is that **WPA-PSK/WPA2-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The NBG420N automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK/ WPA2-PSK** key management) or RADIUS server (if using **WPA/WPA2** key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA-PSK/WPA2-PSK** mode. The default is **1800** seconds (30 minutes).
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.5.4 WPA/WPA2

Click **Network** > **Wireless LAN** to display the **General** screen. Select **WPA** or **WPA2** from the **Security Mode** list.

Figure 65 Network > Wireless LAN > General: WPA/WPA2



The following table describes the labels in this screen.

Table 33 Network > Wireless LAN > General: WPA/WPA2

LABEL	DESCRIPTION
WPA Compatible	This check box is available only when you select **WPA2-PSK** or **WPA2** in the **Security Mode** field. Select the check box to have both WPA2 and WPA wireless clients be able to communicate with the NBG420N even when the NBG420N is using WPA2-PSK or WPA2.
ReAuthentication Timer (in seconds)	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is 1800 seconds (30 minutes). Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout	The NBG420N automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. The default time interval is 3600 seconds (or 1 hour).

Table 33 Network > Wireless LAN > General: WPA/WPA2

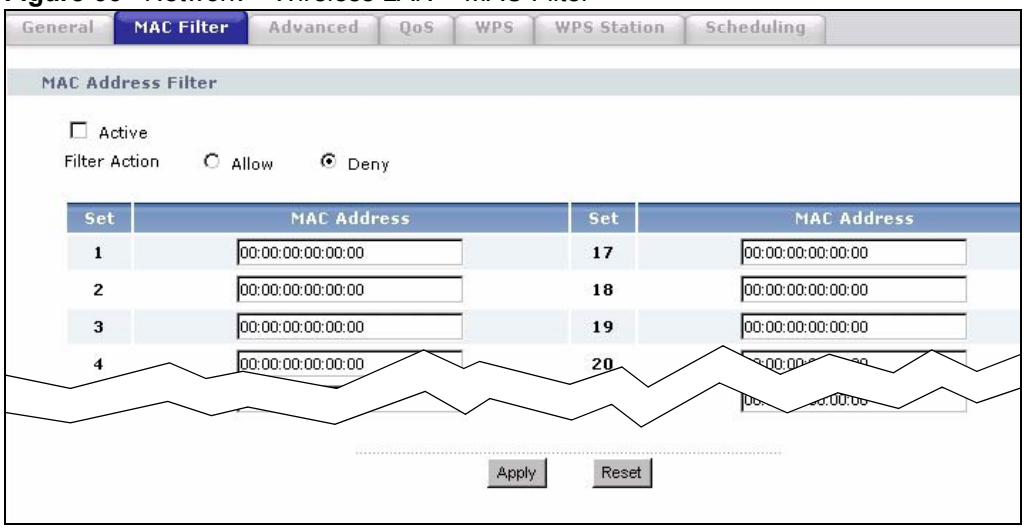
LABEL	DESCRIPTION
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK/ WPA2-PSK** key management) or RADIUS server (if using **WPA/WPA2** key management) sends a new group key out to all clients. The re-keying process is the WPA/WPA2 equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in **WPA-PSK/WPA2-PSK** mode. The NBG420N default is **1800** seconds (30 minutes).
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the NBG420N. The key must be the same on the external authentication server and your NBG420N. The key is not sent over the network.
Accounting Server	
Active	Select **Yes** from the drop down list box to enable user accounting through an external authentication server.
IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	Enter the port number of the external accounting server. The default port number is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the NBG420N. The key must be the same on the external accounting server and your NBG420N. The key is not sent over the network.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.6 MAC Filter

The MAC filter screen allows you to configure the NBG420N to give exclusive access to up to 32 devices (Allow) or exclude up to 32 devices from accessing the NBG420N (Deny). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your NBG420N's MAC filter settings, click **Network** > **Wireless LAN** > **MAC Filter**. The screen appears as shown.

Figure 66 Network > Wireless LAN > MAC Filter



The following table describes the labels in this menu.

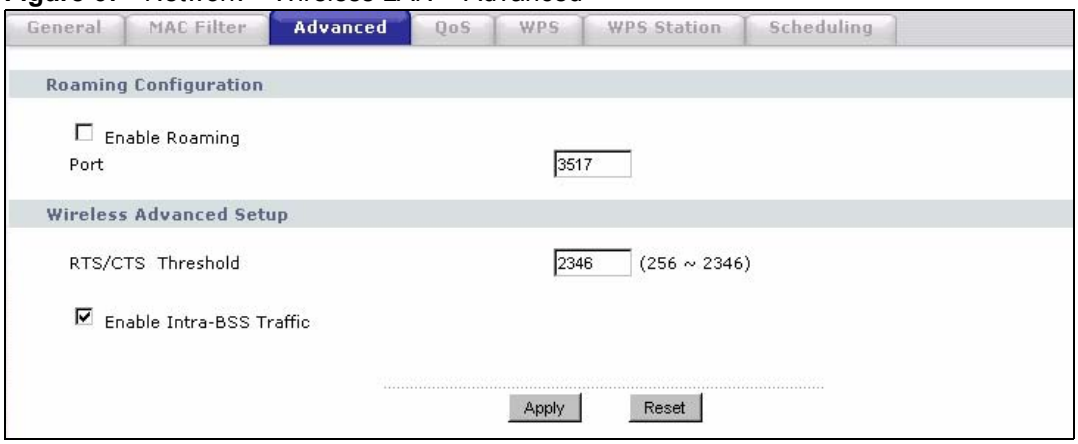
Table 34 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
Active	Select **Yes** from the drop down list box to enable MAC address filtering.
Filter Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny** to block access to the NBG420N, MAC addresses not listed will be allowed to access the NBG420N Select **Allow** to permit access to the NBG420N, MAC addresses not listed will be denied access to the NBG420N.
Set	This is the index number of the MAC address.
MAC Address	Enter the MAC addresses of the wireless station that are allowed or denied access to the NBG420N in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.7 Wireless LAN Advanced Screen

Click **Network** > **Wireless LAN** > **Advanced**. The screen appears as shown.

Figure 67 Network > Wireless LAN > Advanced



The following table describes the labels in this screen.

Table 35 Network > Wireless LAN > Advanced

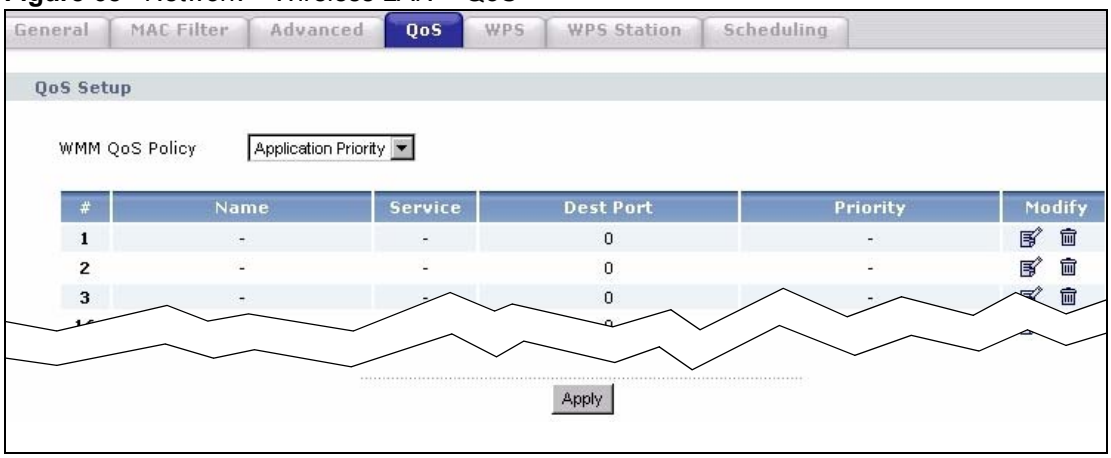
LABEL	DESCRIPTION
Roaming Configuration	
Enable Roaming	Select this option if your network environment has multiple APs and you want your wireless device to be able to access the network as you move between wireless networks.
Wireless Advanced Setup	
RTS/CTS Threshold	Data with its frame size larger than this value will perform the RTS (Request To Send)/CTS (Clear To Send) handshake. Enter a value between 0 and 2432.
Enable Intra-BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.8 Quality of Service (QoS) Screen

The QoS screen allows you to automatically give a service (such as e-mail, VoIP or FTP) a priority level.

Click **Network** > **Wireless LAN** > **QoS**. The following screen appears.

Figure 68 Network > Wireless LAN > QoS



The following table describes the labels in this screen.

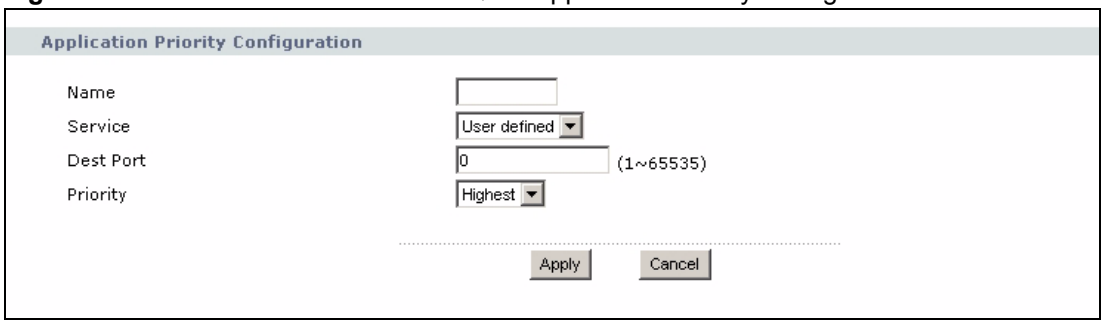
Table 36 Network > Wireless LAN > QoS

LABEL	DESCRIPTION
WMM QoS Policy	Select **Default** to have the NBG420N automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. Select **Application Priority** from the drop-down list box to display a table of application names, services, ports and priorities to which you want to apply WMM QoS.
	The table appears only if you select **Application Priority** in **WMM QoS Policy**.
#	This is the number of an individual application entry.
Name	This field displays a description given to an application entry.
Service	This field displays either **FTP**, **WWW**, **E-mail** or a **User Defined** service to which you want to apply WMM QoS.
Dest Port	This field displays the destination port number to which the application sends traffic.
Priority	This field displays the priority of the application. **Highest** - Typically used for voice or video that should be high-quality. **High** - Typically used for voice or video that can be medium-quality. **Mid** - Typically used for applications that do not fit into another priority. For example, Internet surfing. **Low** - Typically used for non-critical “background” applications, such as large file transfers and print jobs that should not affect other applications.
Modify	Click the **Edit** icon to open the **Application Priority Configuration** screen. Modify an existing application entry or create a application entry in the **Application Priority Configuration** screen. Click the **Remove** icon to delete an application entry.
Apply	Click **Apply** to save your changes to the NBG420N.

7.8.1 Application Priority Configuration

Use this screen to edit a WMM QoS application entry. Click the edit icon under **Modify**. The following screen displays.

Figure 69 Network > Wireless LAN > QoS: Application Priority Configuration



See Appendix F on page 321 for a list of commonly-used services and destination ports. The following table describes the fields in this screen.

Network > Wireless LAN > QoS: Application Priority Configuration

LABEL	DESCRIPTION
Application Priority Configuration	
Name	Type a description of the application priority.
Service	The following is a description of the applications you can prioritize with WMM QoS. Select a service from the drop-down list box. • **E-Mail** Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80 • **FTP** File Transfer Protocol enables fast transfer of files, including large files that it may not be possible to send via e-mail. FTP uses port number 21. • **WWW** The World Wide Web is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser. • **User-Defined** User-defined services are user specific services configured using known ports and applications.
Dest Port	This displays the port the selected service uses. Type a port number in the field provided if you want to use a different port to the default port.
Priority	Select a priority from the drop-down list box.
Apply	Click **Apply** to save your changes back to the NBG420N.
Cancel	Click **Cancel** to return to the previous screen.

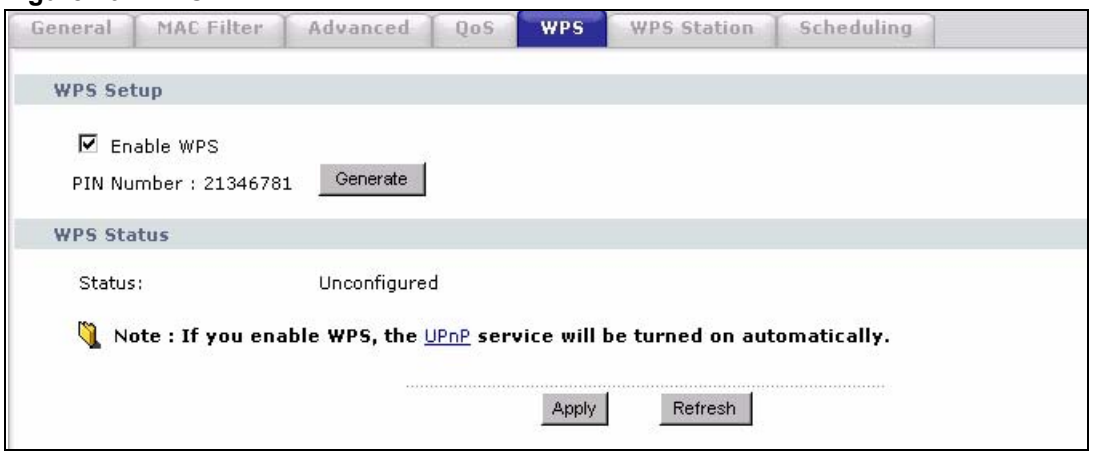
7.9 WiFi Protected Setup

WiFi Protected Setup (WPS) is an industry standard specification, defined by the WiFi Alliance. WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Depending on the devices in your network, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (Personal Identification Number) in the devices. Then, they connect and set up a secure network by themselves. See how to set up a secure wireless network using WPS in the Section 6.1.2 on page 73.

7.9.1 WPS Screen

Use this screen to enable/disable WPS, view or generate a new PIN number and check current WPS status. To open this screen, click **Network** > **Wireless LAN** > **WPS** tab.

Figure 70 WPS



The following table describes the labels in this screen.

Table 37 WPS

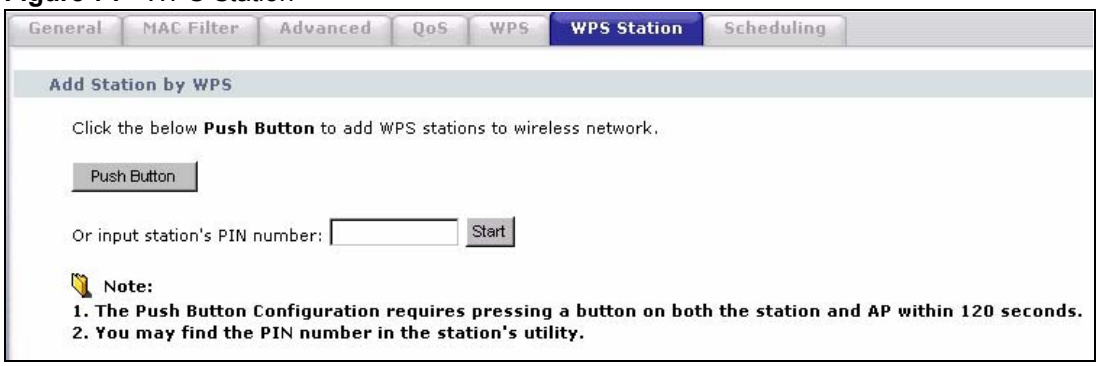
LABEL	DESCRIPTION
WPS Setup	
Enable WPS	Select this to enable the WPS feature.
PIN Number	This displays a PIN number last time system generated. Click **Generate** to generate a new PIN number.
WPS Status	
Status	This displays **Configured** when the NBG420N has connected to a wireless network using WPS or when **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there are no wireless or wireless security changes on the NBG420N or you click **Release_Configuration** to remove the configured wireless and wireless security settings.
Release Configuration	This button is only available when the WPS status displays **Configured**. Click this button to remove all configured wireless and wireless security settings for WPS connections on the NBG420N.
Apply	Click **Apply** to save your changes back to the NBG420N.
Refresh	Click **Refresh** to get this screen information afresh.

7.9.2 WPS Station Screen

Use this screen when you want to add a wireless station using WPS. To open this screen, click **Network** > **Wireless LAN** > **WPS Station** tab.

Note: After you click **Push Button** on this screen, you have to press a similar button in the wireless station utility within 2 minutes. To add the second wireless station, you have to press these buttons on both device and the wireless station again after the first 2 minutes.

Figure 71 WPS Station


General
MAC Filter
Advanced
QoS
WPS
WPS Station
Scheduling
Add Station by WPS
Click the below Push Button to add WPS stations to wireless network.
Push Button
Or input station's PIN number:
Start
Note:
1. The Push Button Configuration requires pressing a button on both the station and AP within 120 seconds.
2. You may find the PIN number in the station's utility.

The following table describes the labels in this screen.

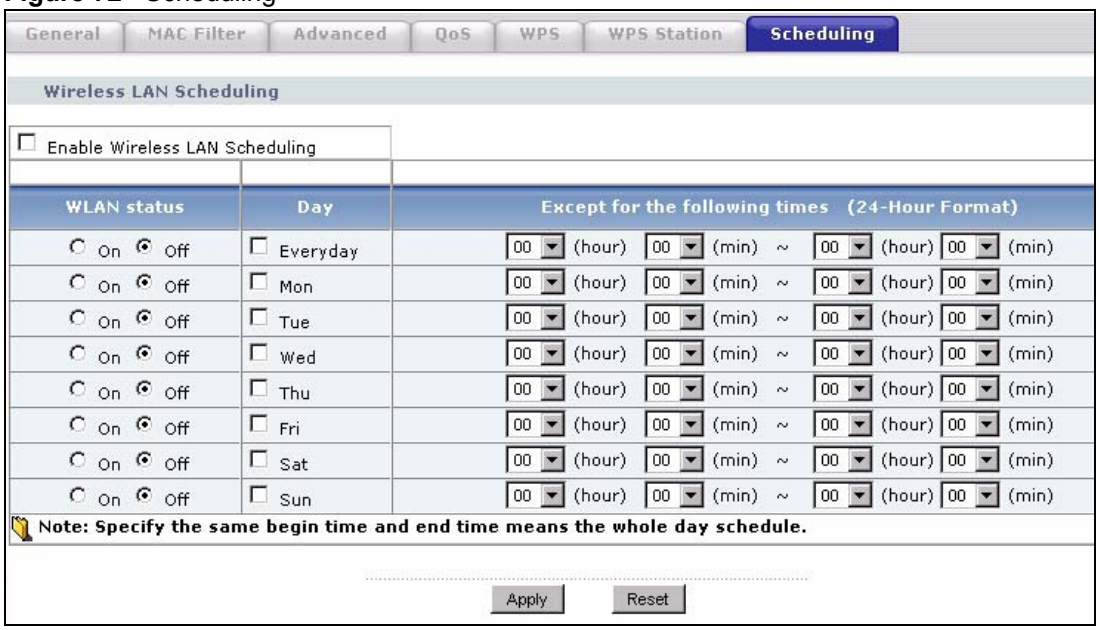
Table 38 WPS Station

LABEL	DESCRIPTION
Push Button	Use this button when you use the PBC (Push Button Configuration) method to configure wireless stations's wireless settings. See Section 6.1.2.1 on page 74. Click this to start WPS-aware wireless station scanning and the wireless security information synchronization.
Or input station's PIN number	Use this button when you use the PIN Configuration method to configure wireless station's wireless settings. See Section 6.1.2.2 on page 75. Type the same PIN number generated in the wireless station's utility. Then click **Start** to associate to each other and perform the wireless security information synchronization.

7.9.3 Scheduling

Use this screen to set the times your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default. The wireless LAN can be scheduled to turn on or off on certain days and at certain times. To open this screen, click **Network** > **Wireless LAN** > **Scheduling** tab.

Figure 72 Scheduling



The following table describes the labels in this screen.

Table 39 Scheduling

LABEL	DESCRIPTION
Enable Wireless LAN Scheduling	Select this to enable Wireless LAN scheduling.
WLAN Status	Select **On** or **Off** to specify whether the Wireless LAN is turned on or off. This field works in conjunction with the **Day** and **Except for the following times** fields.
Day	Select **Everyday** or the specific days to turn the Wireless LAN on or off. If you select **Everyday** you can not select any specific days. This field works in conjunction with the **Except for the following times** field.
Except for the following times (24-Hour Format)	Select a begin time using the first set of **hour** and minute (**min**) drop down boxes and select an end time using the second set of **hour** and minute (**min**) drop down boxes. If you have chosen **On** earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields. If you have chosen **Off** earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. Note: Entering the same begin time and end time will mean the whole day.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to reload the previous configuration for this screen.

7.10 iPod Touch Web Configurator

The iPod Touch web configurator displays when you are connecting to the NBG420N wirelessly with an iPod Touch device through a web browser. It is different to the web configurator that you access from your computer.

To connect wirelessly to the iPod Touch web configurator with your iPod Touch follow the steps below:

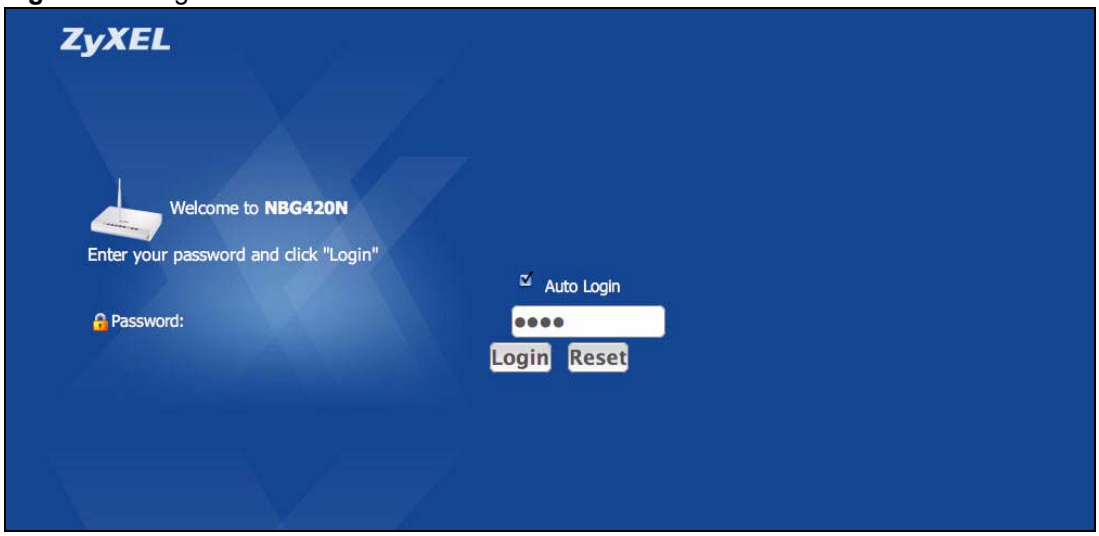
1. Make sure the Wireless LAN on the NBG420N is enabled and that you know the security settings (if any). To do this check the **Wireless LAN > General** screen in the web configurator from your computer.
2. On the iPod Touch's main screen press **Settings > Wi-fi** and from the list press the NBG420N's network name (SSID) to connect to it. If you are prompted for any security settings enter them and press connect. If you cannot connect check your security settings in the web configurator from your computer and try again.
3. After connecting to the NBG420N's wireless LAN network launch the iPod Touch Internet browser and enter the NBG420N's IP address (default: 192.168.1.1) into the address bar. The login screen displays.

7.10.1 Login Screen

After accessing the NBG420N's IP address in the iPod Touch web browser the screen below will display.

You cannot change your password in the iPod Touch web configurator. To change your password log into the web configurator using your computer.

Figure 73 Login Screen



The following table describes the labels in this screen.

Table 40 Login Screen

LABEL	DESCRIPTION
Auto Login	Select this checkbox to automatically log into the iPod Touch web configurator when accessing it through the same iPod Touch device.
Password	Enter the password for the NBG420N. If you haven't changed the default password earlier this is "**1234**".
Login	Press the **Login** button to log into the iPod Touch web configurator.
Reset	Press the **Reset** button to clear your selections and start over.

7.10.2 System Status

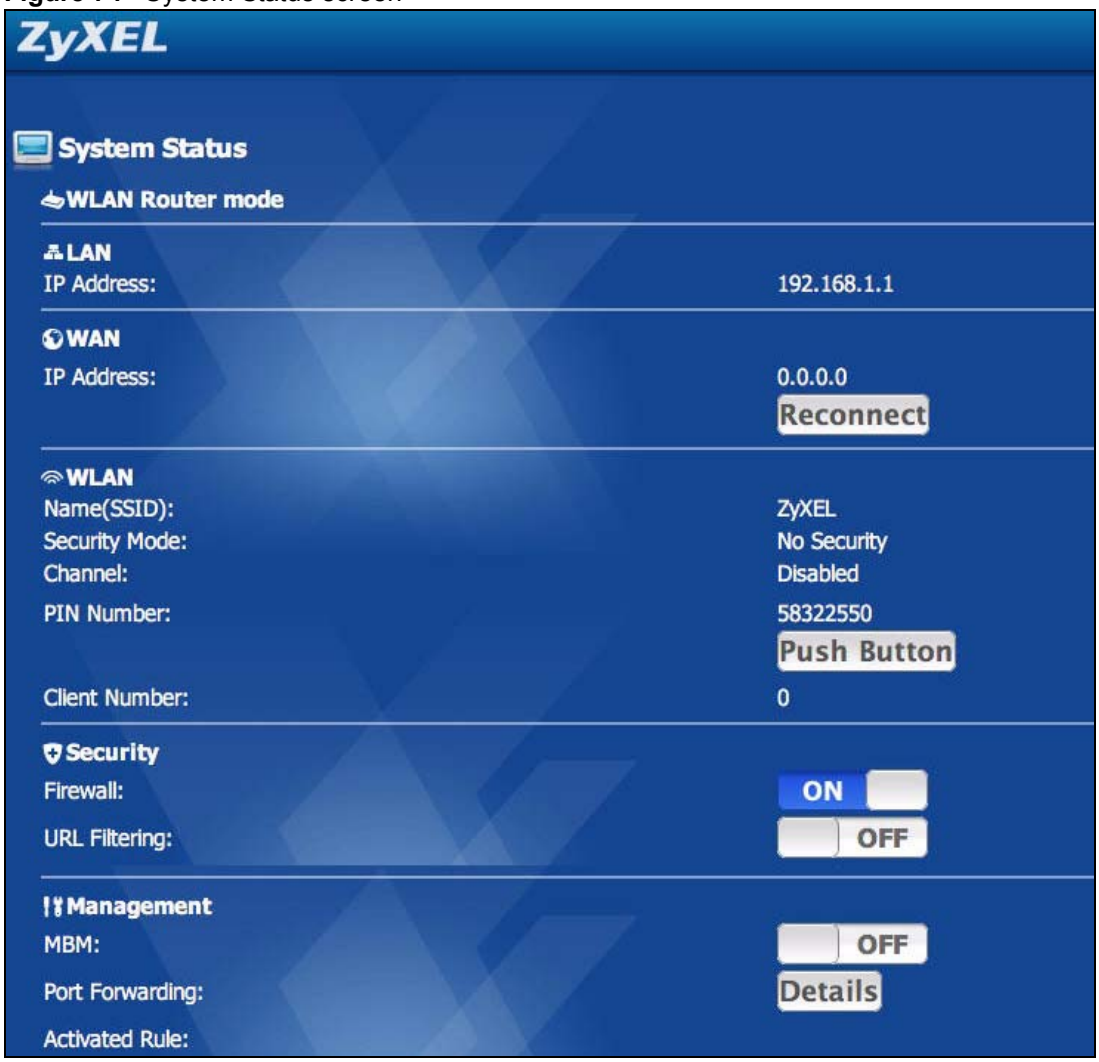
After successfully logging into the iPod Touch web configurator the **System Status** screen displays.

Your changes in the iPod Touch web configurator are saved automatically after pressing a button.

If you are going to use the WPS (Wi-Fi Protected Setup) function in the iPod Touch Web Configurator it is recommended to configure your WPS settings first from your computer.

If WPS has not been configured previously the iPod Touch will lose it's wireless connection to the NBG420N after the NBG420N has connected to another device using WPS through the iPod Touch web configurator. To reconnect to the wireless network using your iPod Touch you must find out the new WPS settings by logging into the web configurator from your computer and going to the **Wireless LAN** screen.

Figure 74 System Status screen



The following table describes the labels in this screen.

Table 41 System Status screen

LABEL	DESCRIPTION
Logout	Press this to logout of the iPod Touch web configurator.
LAN	
IP Address	This field displays the NBG420N's LAN (Local Area Network) IP address.
WAN	
IP Address	This field displays the NBG420N's WAN IP address. If this field displays "**-**" it means the WAN is not connected. Try pressing **Reconnect** if your WAN connection is not working.
Reconnect	Press **Reconnect** to renew your NBG420N's WAN connection.
WLAN	
Name (SSID)	This field displays the SSID (Service set identifier) of the NBG420N's Wireless LAN.
Security Mode	This field displays the security authentication mode of the NBG420N's Wireless LAN. This can be **No Security**, **WPA-PSK**, **WPA2-PSK** or **WEP**.

Table 41 System Status screen

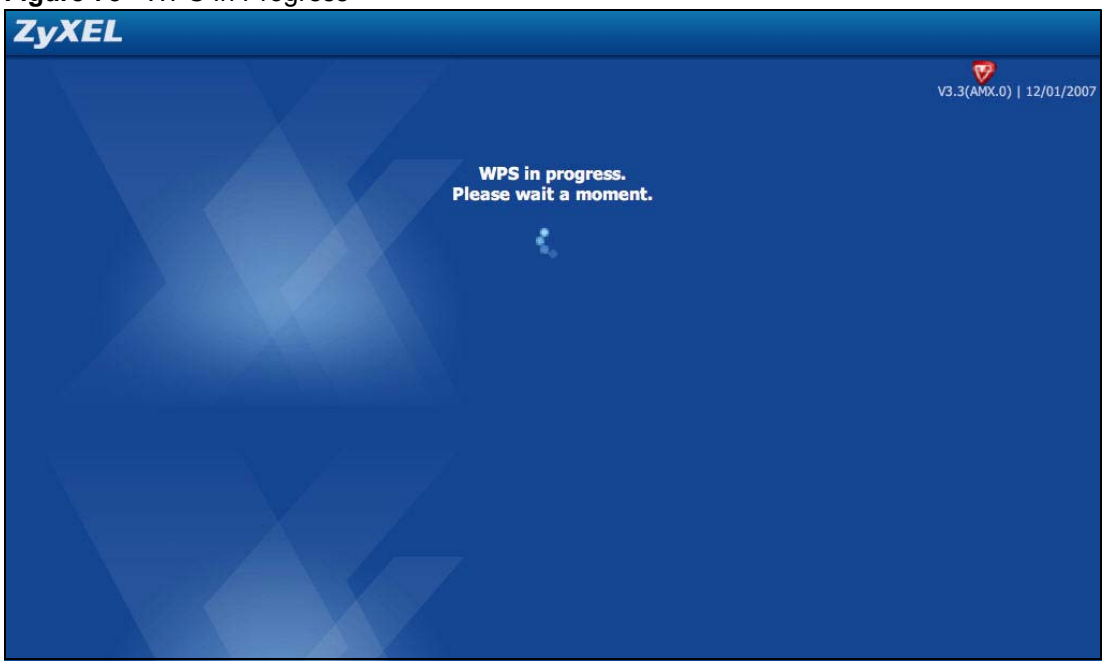
LABEL	DESCRIPTION
Channel	This field displays the channel the NBG420N's Wireless LAN operates on. This will display as disabled if auto channel selection mode is on.
PIN Number	This field displays the NBG420N's WPS (Wi-Fi Protected Setup) PIN number. WPS allows you to connect wireless clients to your wireless LAN easily. See Section 7.9 on page 106 for more information on WPS and the PIN method of configuration.
Push Button	Press the **Push Button** to start either the PBC (Push Button Configuration) or PIN method of WPS configuration. The WPS in progress screen will display, see Section 7.10.3 on page 112.
Client Number	This field displays the number of wireless clients on the network.
Security	
Firewall	Press the left side of the button to turn the firewall **ON**. Press the right side of the button to turn the firewall **OFF**. To configure the firewall access the web configurator from your computer. A Firewall enables the NBG420N to act as a secure gateway between the LAN and the Internet.
URL Filtering	Press the left side of the button to turn URL Filtering **ON**. Press the right side of the button to turn URL Filtering **OFF**. To configure URL filtering access the web configurator from your computer and go to the content filtering screens. Content filtering enables you to block certain web features or specific URL keywords.
Management	
MBM	Press the left side of the button to turn MBM (Media Bandwidth Management) **ON**. Press the right side of the button to turn MBM **OFF**. To configure Media Bandwidth Management access the web configurator from your computer and go to the Bandwidth Management screens. When accessed from a computer the web configurator allows you to specify bandwidth management rules based on an application and/or subnet.
Port Forwarding	Press **Details** to go to another screen to manage the port forwarding rules.
Activated Rule	This field displays the currently activated port forwarding rules.

7.10.3 WPS in Progress

After pressing **Push Button** in the **System Status** screen the WPS in Progress screen will display.

It can take around two minutes for a successful WPS connection to be made. The **System Status** screen will display after a connection has been made or if it has failed. For more information on WPS see Section 7.9 on page 106.

Figure 75 WPS In Progress



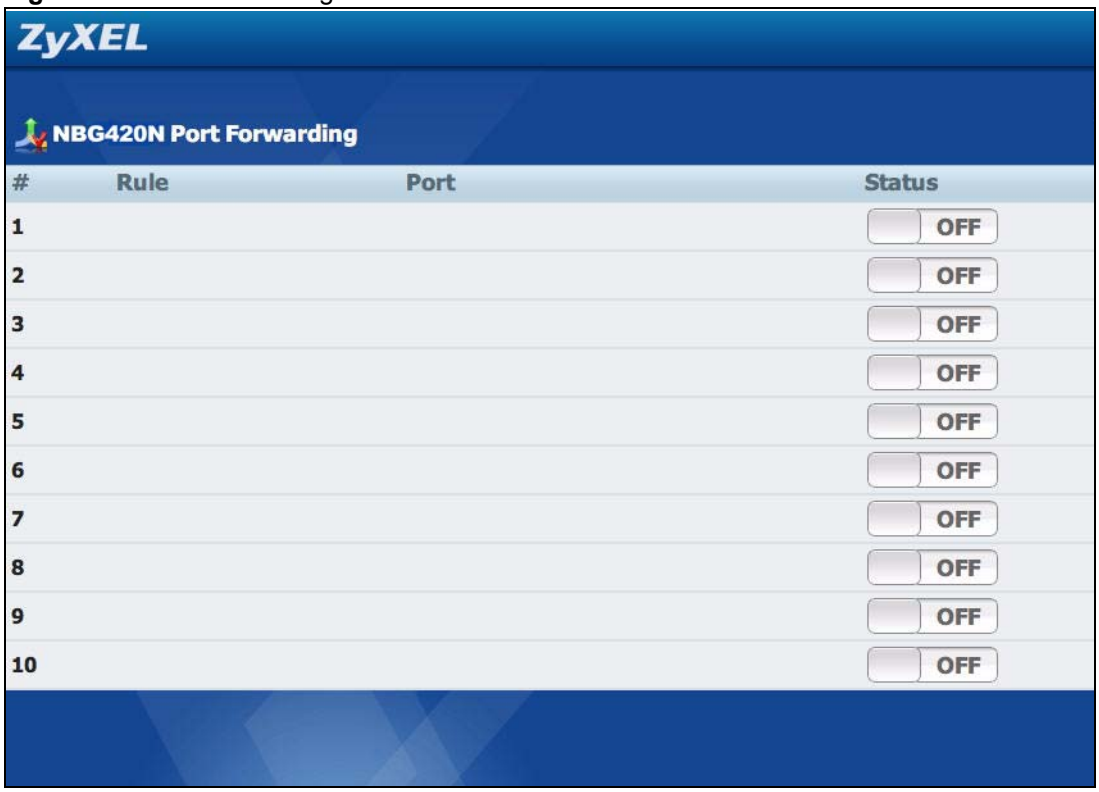
7.10.4 Port Forwarding

After pressing the **Details** button in the **System Status** screen the port forwarding screen will display. Use this screen to change the status of port forwarding rules that have been set up in the web configurator from your computer. See Section 11.4 on page 139 for more information on configuring port forwarding rules.

To go back to the **System Status** screen press the ZyXEL logo at the top of the page.

To see any changes on the **System Status** screen you will need to refresh the page first. Use the browser's refresh function. See the iPod Touch's documentation if you cannot find it.

Figure 76 Port Forwarding



The following table describes the labels in this screen.

Table 42 Port Forwarding

LABEL	DESCRIPTION
#	This is the number of an individual port forwarding entry.
Rule	This column displays the configured port forwarding rules. To configure a new rule you must use the web configurator from your computer.
Port	This column displays the port number(s) which are forwarded when the rule is turned on.
Status	Use this column to manage the status of the rules. Press the left side of the button to turn the rule **ON** and press the right side of the button to turn the rule **OFF**.

7.11 Accessing the iPod Touch Web Configurator

To access the iPod Touch web configurator through your iPod Touch you must first connect it to the NBG420N's wireless network. Follow the steps below to do this.

If you have not configured your wireless settings yet you can do so by using the Wizard in the web configurator you access from your computer. Click the Wizard icon or the **Go To Wizard Setup** web link you see after logging into the web configurator from your computer. See Chapter 4 on page 49 for more information on using the Wizard.

1 On the iPod Touch's main screen press **Settings** and then press **Wi-fi**.
2 On the list of networks press the NBG420N's network name (SSID) to connect to it. If you are prompted for any security settings enter them and press connect.

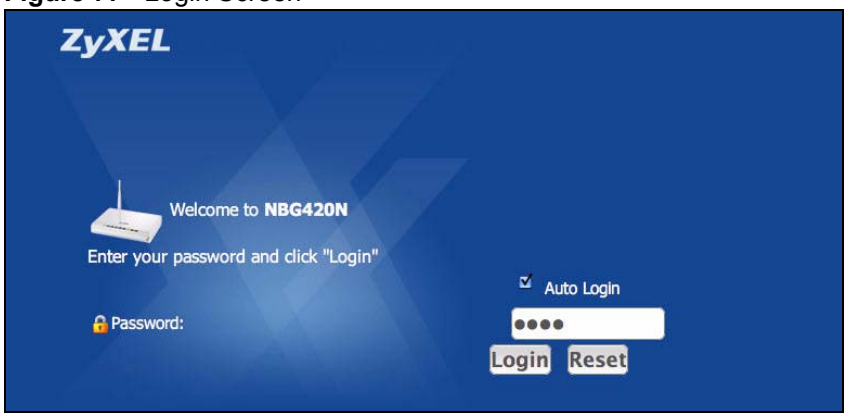
The pre-shared key is case-sensitive. If you have problems connecting then try checking the security settings in the web configurator from your computer and try again.

7.11.1 Accessing the iPod Touch Web Configurator

Now that you are connected to the NBG420N's wireless network you can access the iPod Touch web configurator. To do this follow the steps below:

1 Launch the iPod Touch's web browser from the main screen. The default web browser is Safari.
2 Enter the IP address of the NBG420N into the address bar and go to that address. The default IP address for the NBG420N is 192.168.1.1.
3 The login screen should display.

Figure 77 Login Screen



If the login screen does not display properly, check that you are accessing the correct IP address. Also check your iPod Touch web browser's security settings as they may affect how the page displays.

4 If you wish to login automatically in the future make sure the **Auto Login** checkbox is selected.
5 Enter your password and press login. The default password for the NBG420N is "**1234**".
6 The **System Status** screen will display after successfully logging in. Congratulations! For information on using the configurator see Section 7.10 on page 108.

8

WAN

This chapter describes how to configure WAN settings.

8.1 WAN Overview

See the chapter about the connection wizard for more information on the fields in the WAN screens.

8.2 WAN MAC Address

The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. It is recommended that you clone the MAC address prior to hooking up the WAN Port.

8.3 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The NBG420N supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the NBG420N queries all directly connected networks to gather group membership. After that, the NBG420N periodically updates this information. IP multicasting can be enabled/disabled on the NBG420N LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

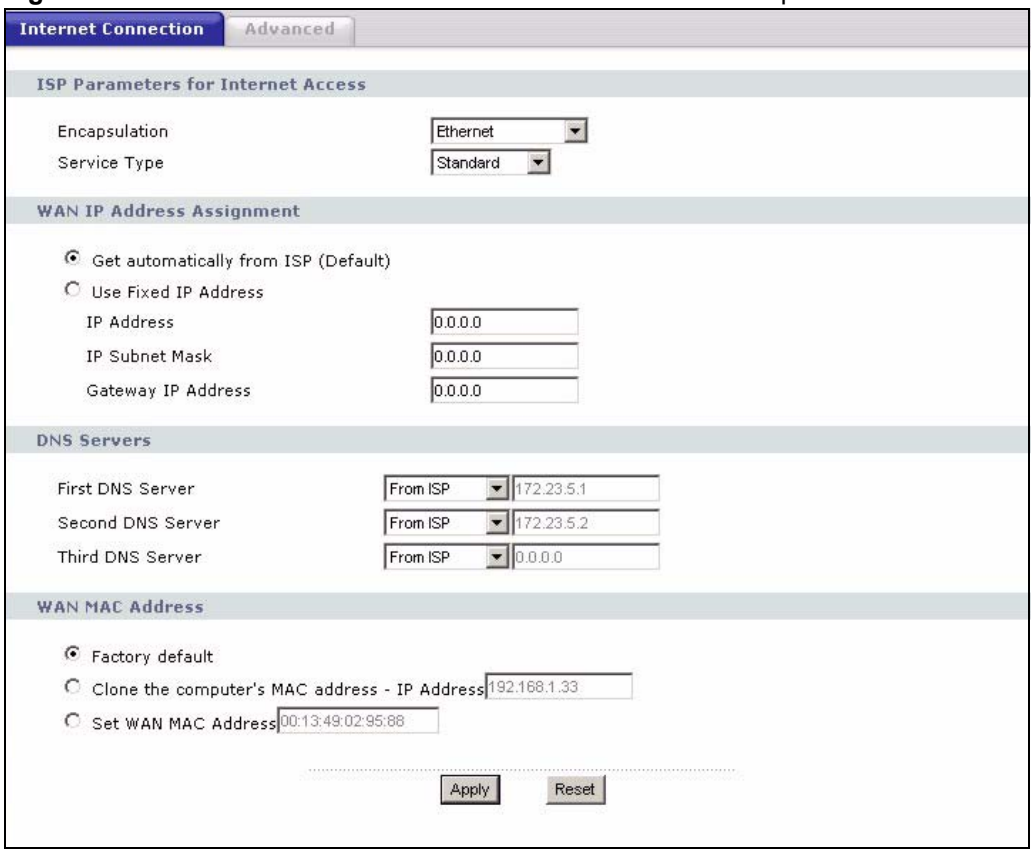
8.4 Internet Connection

Use this screen to change your NBG420N's Internet access settings. Click **Network** > **WAN**. The screen differs according to the encapsulation you choose.

8.4.1 Ethernet Encapsulation

This screen displays when you select **Ethernet** encapsulation.

Figure 78 Network > WAN > Internet Connection: Ethernet Encapsulation



The following table describes the labels in this screen.

Table 43 Network > WAN > Internet Connection: Ethernet Encapsulation

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from **Standard**, **RR-Telstra** (RoadRunner Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Toshiba** (Roadrunner Toshiba authentication method) or **Telia Login**. The following fields do not appear with the **Standard** service type.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
IP Subnet Mask	Enter the **IP Subnet Mask** in this field.
Gateway IP Address	Enter a **Gateway IP Address** (if your ISP gave you one) in this field.
DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG420N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG420N's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

8.4.2 PPPoE Encapsulation

The NBG420N supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPP over Ethernet** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius).

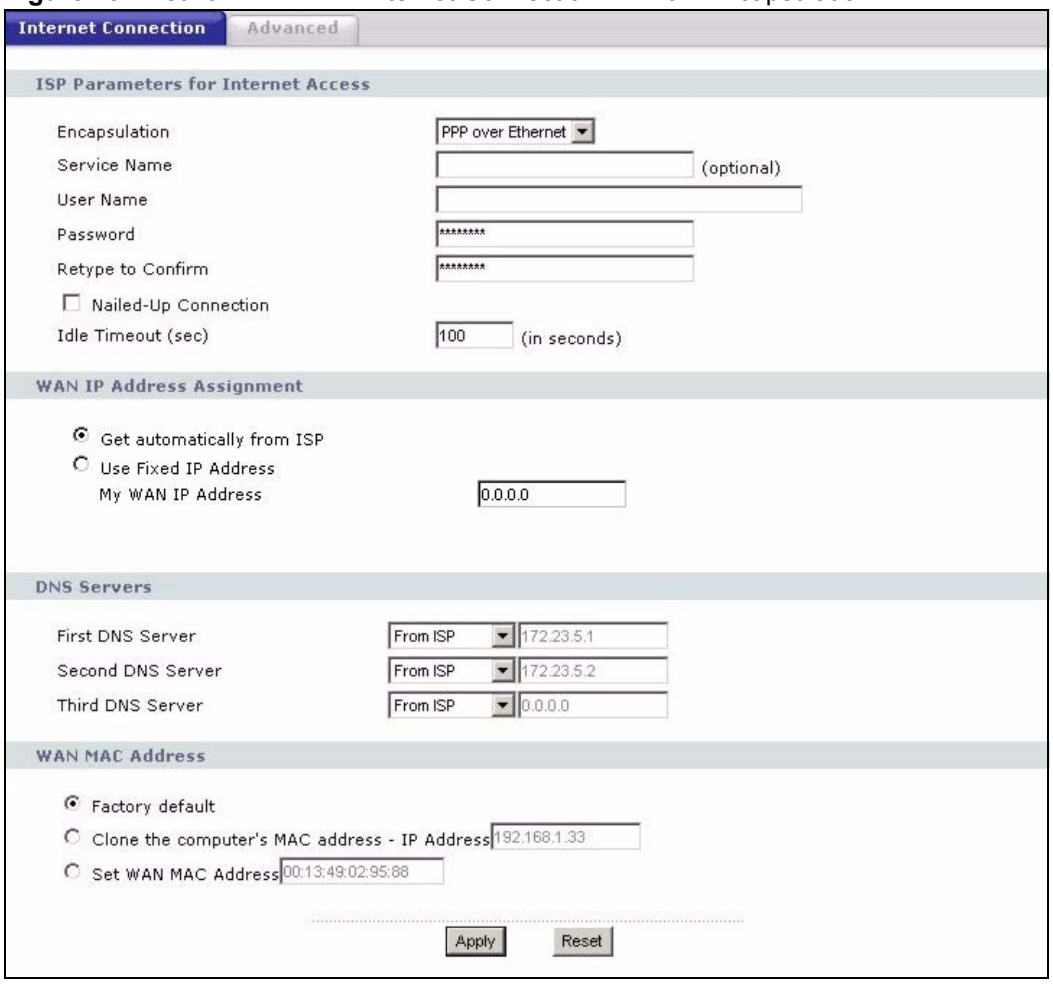
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the NBG420N (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the NBG420N does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

This screen displays when you select **PPPoE** encapsulation.

Figure 79 Network > WAN > Internet Connection: PPPoE Encapsulation



The following table describes the labels in this screen.

Table 44 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The **PPP over Ethernet** choice is for a dial-up connection using PPPoE. The NBG420N supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-Up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG420N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by using the NBG420N's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.

Table 44 Network > WAN > Internet Connection: PPPoE Encapsulation

LABEL	DESCRIPTION
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

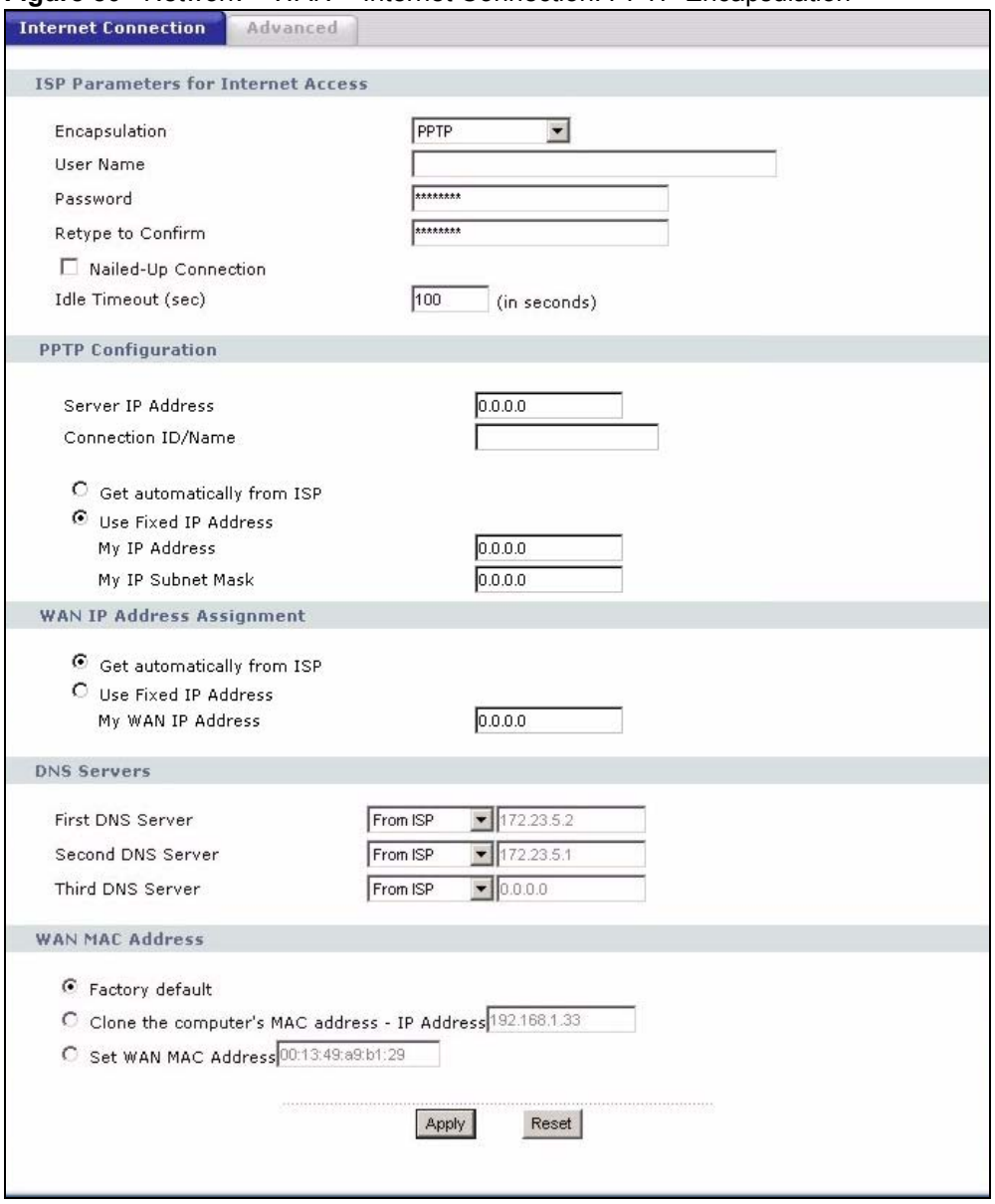
8.4.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

This screen displays when you select **PPTP** encapsulation.

Figure 80 Network > WAN > Internet Connection: PPTP Encapsulation



The following table describes the labels in this screen.

Table 45 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The NBG420N supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.

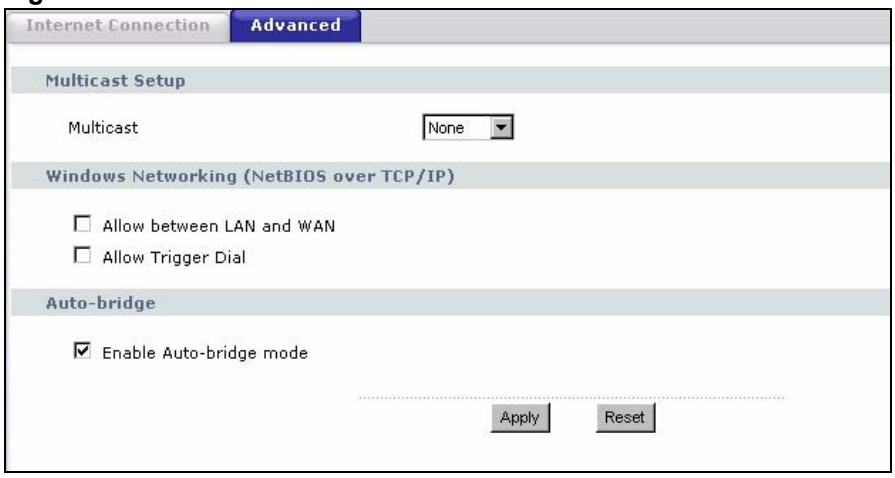
Table 45 Network > WAN > Internet Connection: PPTP Encapsulation

LABEL	DESCRIPTION
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-up Connection	Select **Nailed-Up Connection** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the NBG420N automatically disconnects from the PPTP server.
PPTP Configuration	
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Type your identification name for the PPTP server.
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Your NBG420N will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the NBG420N.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address**.
DNS Servers	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG420N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
WAN MAC Address	The MAC address section allows users to configure the WAN port's MAC address by either using the NBG420N's MAC address, copying the MAC address from a computer on your LAN or manually entering a MAC address.
Factory default	Select **Factory default** to use the factory assigned default MAC Address.
Clone the computer's MAC address	Select **Clone the computer's MAC address - IP Address** and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.
Set WAN MAC Address	Select this option and enter the MAC address you want to use.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

8.5 Advanced WAN Screen

To change your NBG420N's advanced WAN settings, click **Network** > **WAN** > **Advanced**. The screen appears as shown.

Figure 81 Network > WAN > Advanced



The following table describes the labels in this screen.

Table 46 WAN > Advanced

LABEL	DESCRIPTION
Multicast Setup	
Multicast	Select **IGMP V-1**, **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.

Table 46 WAN > Advanced

LABEL	DESCRIPTION
Enable Auto-bridge mode	Select this option to have the NBG420N switch to bridge mode automatically when the NBG420N gets a WAN IP address in the range of 192.168.x.y (where x and y are from zero to nine) no matter what the LAN IP address is. This might happen if you put the NBG420N behind a NAT router that assigns it this IP address. When the NBG420N is in bridge mode, the NBG420N acts as an AP and all the interfaces (LAN, WAN and WLAN) are bridged. In this mode, your NAT, DHCP server, firewall and bandwidth management (rules) on the NBG420N are not available. You do not have to reconfigure them if you return to router mode. Note: The NBG420N automatically turns back to **Router Mode** when the NBG420N gets a WAN IP address that is not in the 192.168.x.y range. Auto-bridging only works under the following conditions: • The WAN IP must be 192.168.x.y (where x and y must be from zero to nine). If the LAN IP address and the WAN IP address are in the same subnet but x or y is greater than nine, the device operates in router mode (with firewall and bandwidth management available). • The device must be in **Router Mode** (see Chapter 24 on page 259 for more information) for auto-bridging to become active.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

9 LAN

This chapter describes how to configure LAN settings.

9.1 LAN Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

9.1.1 IP Pool Setup

The NBG420N is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the NBG420N itself) in the lower range (192.168.1.2 to 192.168.1.32) for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

9.1.2 System DNS Servers

Refer to the IP address and subnet mask section in the **Connection Wizard** chapter.

9.2 LAN TCP/IP

The NBG420N has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

9.2.1 Factory LAN Defaults

The LAN parameters of the NBG420N are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

9.2.2 IP Address and Subnet Mask

Refer to the IP address and subnet mask section in the **Connection Wizard** chapter for this information.

9.2.3 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The NBG420N supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the NBG420N queries all directly connected networks to gather group membership. After that, the NBG420N periodically updates this information. IP multicasting can be enabled/disabled on the NBG420N LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

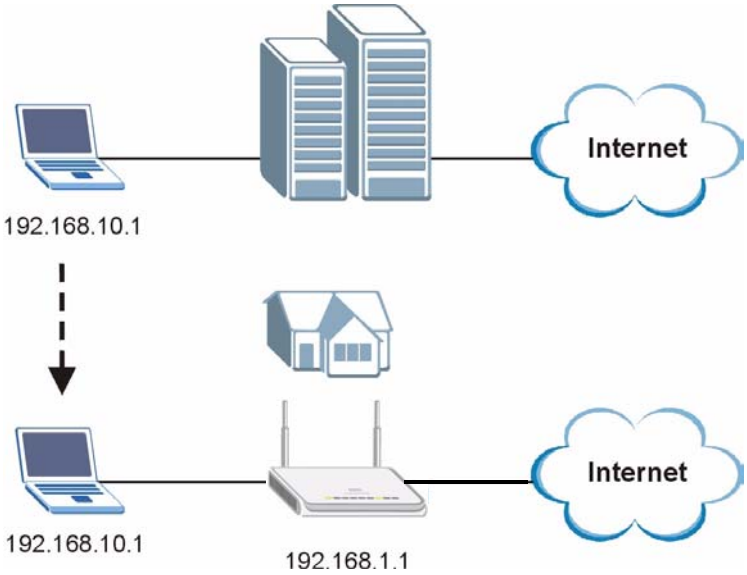
9.2.4 Any IP

Traditionally, you must set the IP addresses and the subnet masks of a computer and the NBG420N to be in the same subnet to allow the computer to access the Internet (through the NBG420N). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the NBG420N.

With the Any IP feature and NAT enabled, the NBG420N allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the NBG420N are not in the same subnet. Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the NBG420N and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a NBG420N is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the NBG420N are not in the same subnet.

Figure 82 Any IP Example



The Any IP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the NBG420N's IP address.

You *must* enable NAT to use the Any IP feature on the NBG420N.

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. IP routing table is defined on IP Ethernet devices (the NBG420N) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the NBG420N.

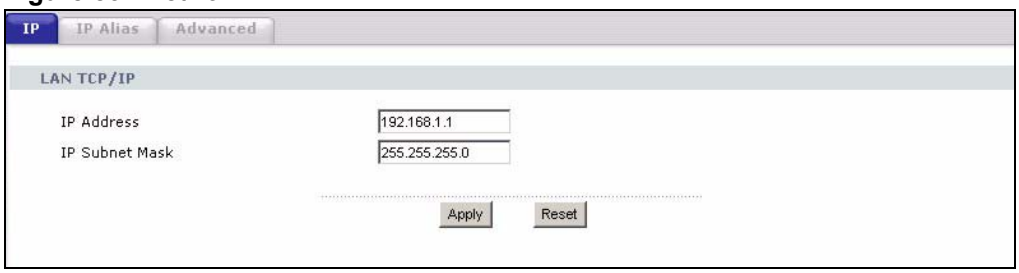
1. When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the NBG420N) by looking at the MAC address in its ARP table.
2. When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.
3. The NBG420N receives the ARP request and replies to the computer with its own MAC address.
4. The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the NBG420N.
5. When the NBG420N receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

After all the routing information is updated, the computer can access the NBG420N and the Internet as if it is in the same subnet as the NBG420N.

9.3 LAN IP Screen

Use this screen to change your basic LAN settings. Click **Network** > **LAN**.

Figure 83 Network > LAN > IP



The following table describes the labels in this screen.

Table 47 Network > LAN > IP

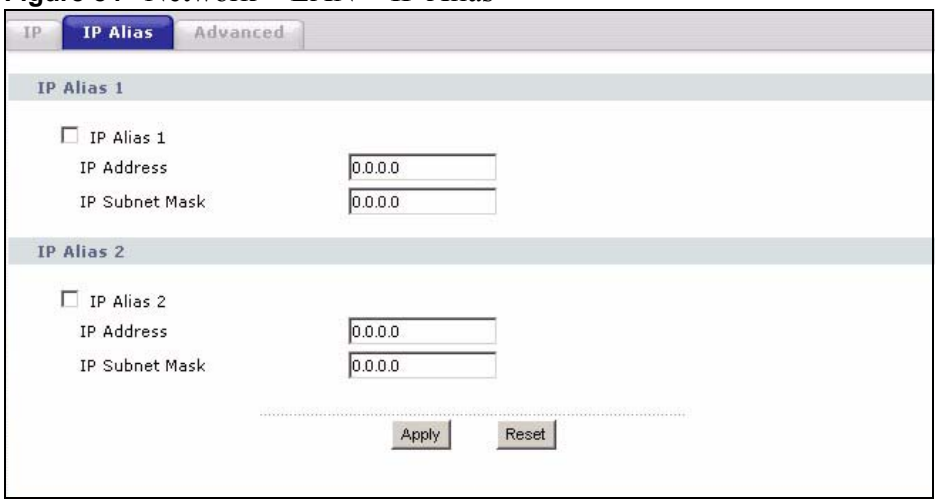
LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Type the IP address of your NBG420N in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your NBG420N will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the NBG420N.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

9.4 LAN IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The NBG420N supports three logical LAN interfaces via its single physical Ethernet interface with the NBG420N itself as the gateway for each LAN network.

To change your NBG420N's IP alias settings, click **Network** > **LAN** > **IP Alias**. The screen appears as shown.

Figure 84 Network > LAN > IP Alias



The following table describes the labels in this screen.

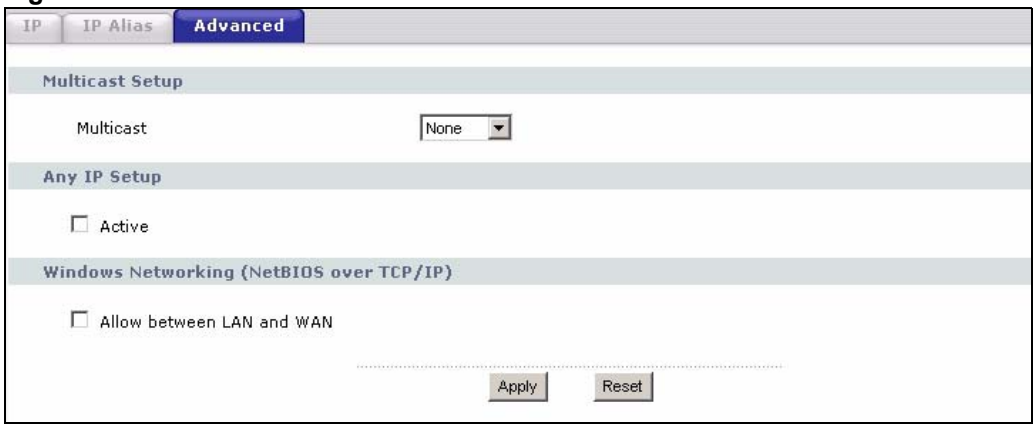
Table 48 Network > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias 1,2	Select the check box to configure another LAN network for the NBG420N.
IP Address	Enter the IP address of your NBG420N in dotted decimal notation.
IP Subnet Mask	Your NBG420N will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the NBG420N.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

9.5 Advanced LAN Screen

To change your NBG420N's advanced IP settings, click **Network** > **LAN** > **Advanced**. The screen appears as shown.

Figure 85 Network > LAN > Advanced



The following table describes the labels in this screen.

Table 49 Network > LAN > Advanced

LABEL	DESCRIPTION
Multicast	Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Any IP Setup	
Active	Select this if you want to let computers on different subnets use the NBG420N.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

10 DHCP

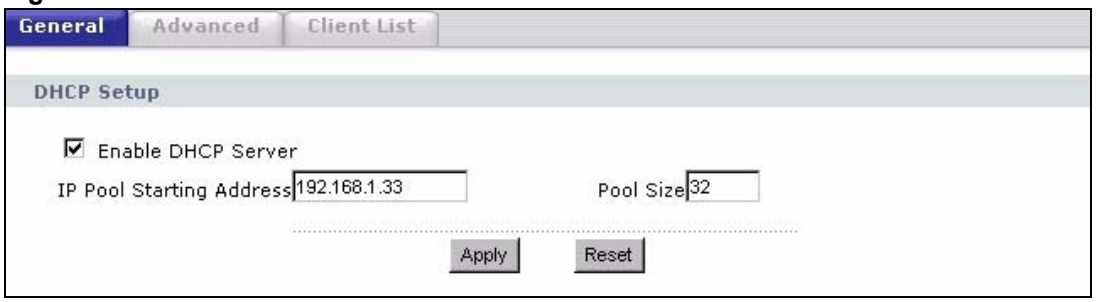
10.1 DHCP

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the NBG420N's LAN as a DHCP server or disable it. When configured as a server, the NBG420N provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

10.2 DHCP General Screen

Click **Network** > **DHCP**. The following screen displays.

Figure 86 Network > DHCP > General



The following table describes the labels in this screen.

Table 50 Network > DHCP > General

LABEL	DESCRIPTION
LAN DHCP Setup	
Enable DHCP Server	Enable or Disable DHCP for LAN. DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Leave the **Enable DHCP Server** check box selected unless your ISP instructs you to do otherwise. Clear it to disable the NBG420N acting as a DHCP server. When configured as a server, the NBG420N provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool for LAN.
Pool Size	This field specifies the size, or count of the IP address pool for LAN.

Table 50 Network > DHCP > General

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

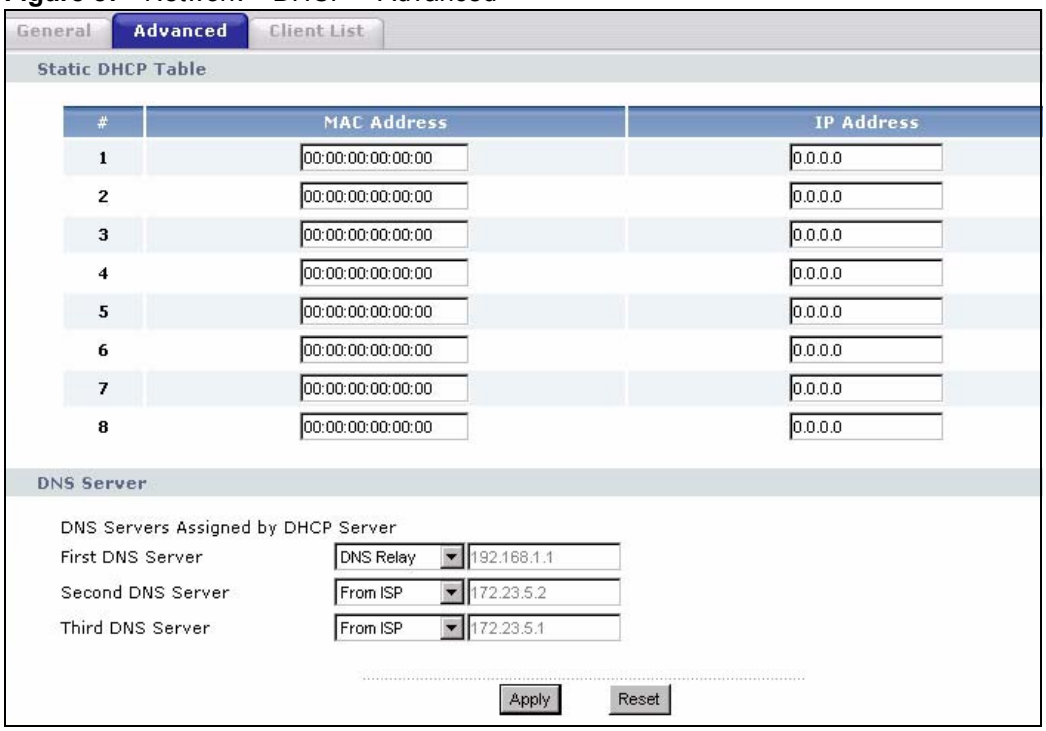
10.3 DHCP Advanced Screen

This screen allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses. You can also use this screen to configure the DNS server information that the NBG420N sends to the DHCP clients.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

To change your NBG420N's static DHCP settings, click **Network** > **DHCP** > **Advanced**. The following screen displays.

Figure 87 Network > DHCP > Advanced



The following table describes the labels in this screen.

Table 51 Network > DHCP > Advanced

LABEL	DESCRIPTION
Static DHCP Table	
#	This is the index number of the static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	Type the LAN IP address of a computer on your LAN.

Table 51 Network > DHCP > Advanced

LABEL	DESCRIPTION
DNS Server	
DNS Servers Assigned by DHCP Server	The NBG420N passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The NBG420N only passes this information to the LAN DHCP clients when you select the **Enable DHCP Server** check box. When you clear the **Enable DHCP Server** check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the NBG420N's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **DNS Relay** to have the NBG420N act as a DNS proxy. The NBG420N's LAN IP address displays in the field to the right (read-only). The NBG420N tells the DHCP clients on the LAN that the NBG420N itself is the DNS server. When a computer on the LAN sends a DNS query to the NBG420N, the NBG420N forwards the query to the NBG420N's system DNS server (configured in the **WAN > Internet Connection** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select **DNS Relay** for a second or third DNS server, that choice changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

10.4 Client List Screen

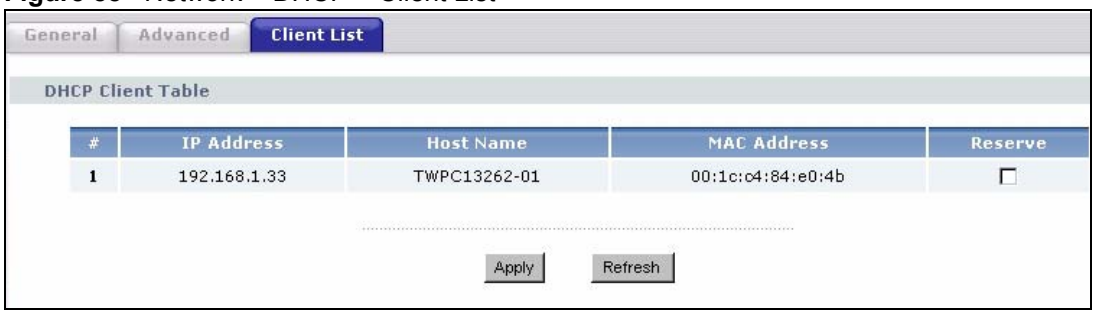
The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of network clients using the NBG420N's DHCP servers.

Configure this screen to always assign an IP address to a MAC address (and host name). Click **Network** > **DHCP Server** > **Client List**.

You can also view a read-only client list by clicking the **DHCP Table (Details...)** hyperlink in the **Status** screen.

The following screen displays.

Figure 88 Network > DHCP > Client List



The following table describes the labels in this screen.

Table 52 Network > DHCP > Client List

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select this check box in the **DHCP Setup** section to have the NBG420N always assign the IP address(es) to the MAC address(es) (and host name(s)). After you click **Apply**, the MAC address and IP address also display in the **Advanced** screen (where you can edit them).
Apply	Click **Apply** to save your settings.
Refresh	Click **Refresh** to reload the DHCP table.

11

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the NBG420N.

11.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

11.2 Using NAT

You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the NBG420N.

11.2.1 Port Forwarding: Services and Port Numbers

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use the **Application** screen to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

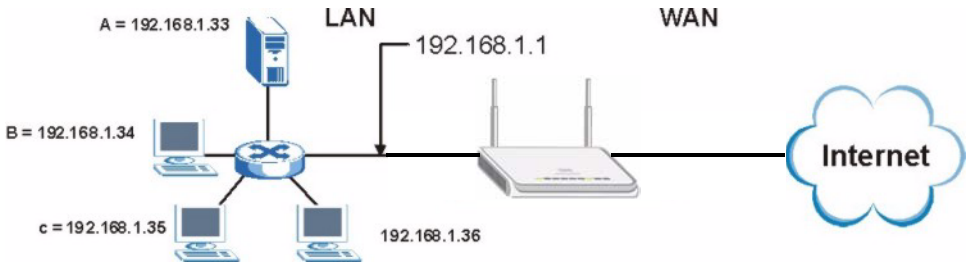
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

11.2.2 Configuring Servers Behind Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

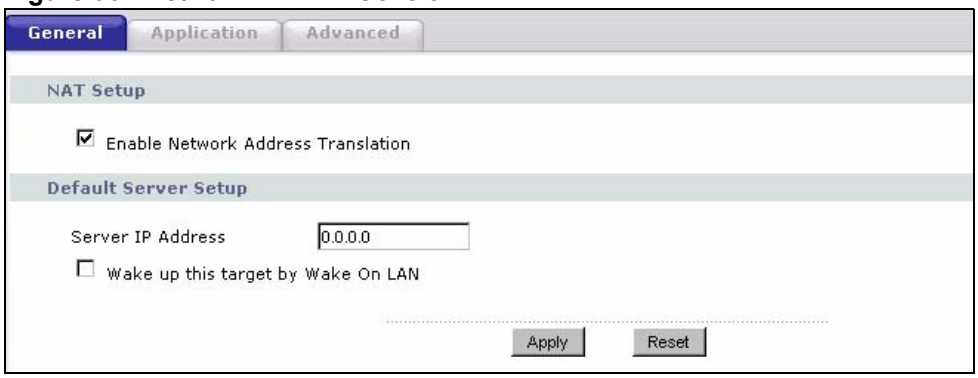
Figure 89 Multiple Servers Behind NAT Example



11.3 General NAT Screen

Click **Network > NAT** to open the **General** screen.

Figure 90 Network > NAT > General



The following table describes the labels in this screen.

Table 53 Network > NAT > General

LABEL	DESCRIPTION
Enable Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select the check box to enable NAT.
Default Server Setup	
Server IP Address	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in the **Application** screen. If you do not assign a **Default Server IP address**, the NBG420N discards all packets received for ports that are not specified in the **Application** screen or remote management.
Wake up this target by Wake On LAN	Select this to use WoL (Wake On LAN) to turn on the server specified in the **Server IP Address** field when packets are received on ports not specified in the **Application** screen. Note: For more information on Wake On LAN see Section 22.4 on page 255.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

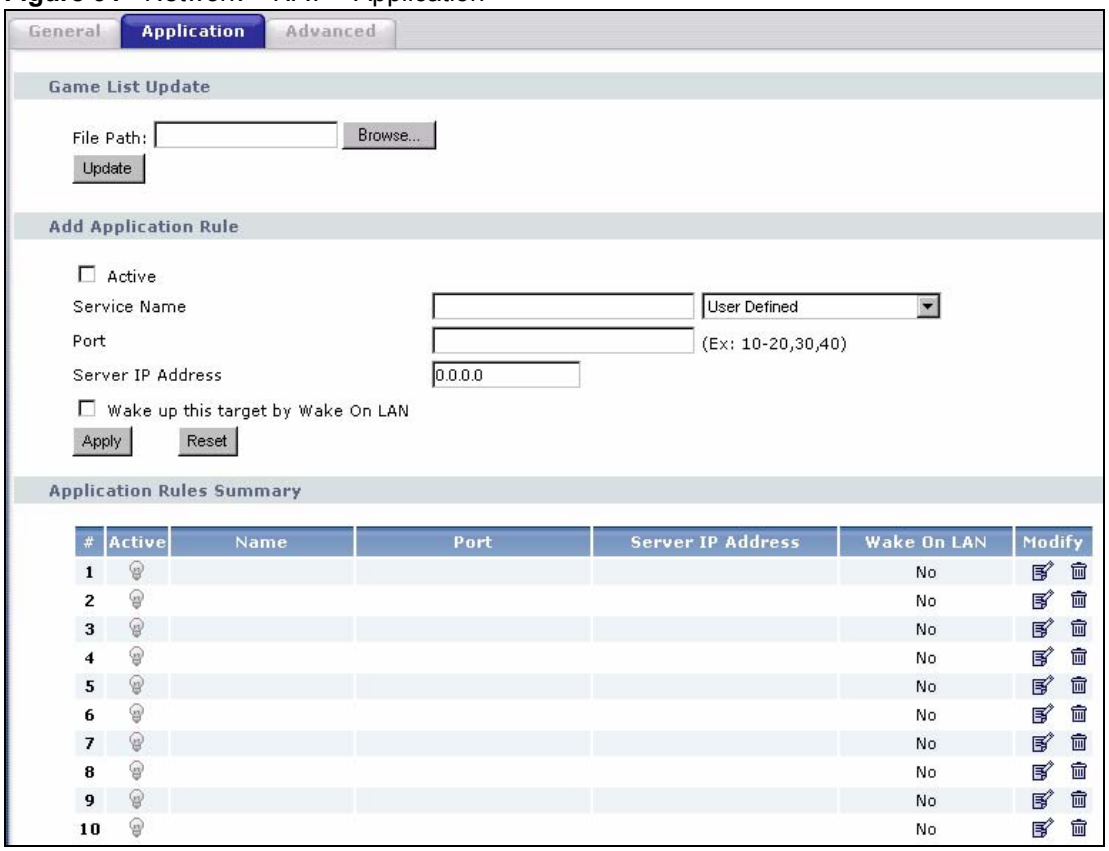
11.4 NAT Application Screen

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your NBG420N's port forwarding settings, click **Network > NAT** > **Application**. The screen appears as shown.

If you do not assign a **Default Server IP address** in the **NAT > General** screen, the NBG420N discards all packets received for ports that are not specified in this screen or remote management.

Refer to Appendix F on page 321 for port numbers commonly used for particular services.

Figure 91 Network > NAT > Application



The following table describes the labels in this screen.

Table 54 NAT Application

LABEL	DESCRIPTION
Game List Update	A game list includes the pre-defined service name(s) and port number(s). You can edit and upload it to the NBG420N to replace the existing entries in the second field next to **Service Name**.
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the.txt file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Update	Click **Update** to begin the upload process. This process may take up to two minutes.
Add Application Rule	
Active	Select the check box to enable this rule and the requested service can be forwarded to the host with a specified internal IP address. Clear the checkbox to disallow forwarding of these ports to an inside server without having to delete the entry.
Service Name	Type a name (of up to 31 printable characters) to identify this rule in the first field next to **Service Name**. Otherwise, select a predefined service in the second field next to **Service Name**. The predefined service name and port number(s) will display in the **Service Name** and **Port** fields.

Table 54 NAT Application (continued)

LABEL	DESCRIPTION
Port	Type a port number(s) to be forwarded. To specify a range of ports, enter a hyphen (-) between the first port and the last port, such as 10-20. To specify two or more non-consecutive port numbers, separate them by a comma without spaces, such as 123,567.
Server IP Address	Type the inside IP address of the server that receives packets from the port(s) specified in the **Port** field.
Wake up this target by Wake On LAN	Select this to use WoL (Wake On LAN) to turn on the server specified in the **IP address** field when packets are received on the ports specified in the **Port** field. Note: For more information on Wake On LAN see Section 22.4 on page 255.
Apply	Click **Apply** to save your changes to the **Application Rules Summary** table.
Reset	Click **Reset** to not save and return your new changes in the **Service Name** and **Port** fields to the previous one.
Application Rules Summary	
#	This is the number of an individual port forwarding server entry.
Active	This icon is turned on when the rule is enabled.
Name	This field displays a name to identify this rule.
Port	This field displays the port number(s).
Server IP Address	This field displays the inside IP address of the server.
Wake On LAN	This field displays **No** when **Wake On LAN** is disabled and **Yes** when **Wake On LAN** is enabled.
Modify	Click the **Edit** icon to display and modify an existing rule setting in the fields under **Add Application Rule**. Click the **Remove** icon to delete a rule.

11.4.1 Game List Example

Here is an example game list text file. The index number, service name and associated port(s) are specified by semi-colons (no spaces). Use the name=xxx (where xxx is the service name) to create a new service. Port range can be separated with a hyphen (-) (no spaces). Multiple (non-consecutive) ports can be separated by commas.

Figure 92 Game List Example

```
version=1
1;name=Battlefield 1942;port=14567,22000,23000-23009,27900,28900
2;name=Call of Duty;port=28960
3;name=Civilization IV;port=2056
4;name=Diablo I and II;port=6112-6119,4000
5;name=Doom 3;port=27666
6;name=F.E.A.R;port=27888
7;name=Final Fantasy XI;port=25,80,110,443,50000-65535
8;name=Guild Wars;port=6112,80
9;name=Half Life;port=6003,7002,27005,27010,27011,27015
10;name=Jedi Knight III: Jedi Academy;port=28060-28062,28070-28081
11;name=Need for Speed: Hot Pursuit 2;port=1230,8511-
8512,27900,28900,61200-61230
12;name=Neverwinter Nights;port=5120-5300,6500,27900,28900
13;name=Quake 2;port=27910
14;name=Quake 3;port=27660,27960
15;name=Rainbow Six 3: Raven Shield;port=7777-7787,8777-8787
16;name=Serious Sam II;port=25600-25605
17;name=Silent Hunter III;port=17997-18003
18;name=Soldier of Fortune II;port=20100-20112
19;name=Starcraft;port=6112-6119,4000
20;name=Star Trek: Elite Force II;port=29250,29256
21;name=SWAT 4;port=10480-10483
22;name=Warcraft II and III;port=6112-6119,4000
23;name=World of Warcraft;port=3724
```

11.5 Trigger Port Forwarding

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The NBG420N records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the NBG420N's WAN port receives a response with a specific port number and protocol ("incoming" port), the NBG420N forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

11.5.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

Figure 93 Trigger Port Forwarding Process: Example

1. Jane requests a file from the Real Audio server (port 7070).
2. Port 7070 is a "trigger" port and causes the NBG420N to record Jane's computer IP address. The NBG420N associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3. The Real Audio server responds using a port number ranging between 6970-7170.
4. The NBG420N forwards the traffic to Jane's computer IP address.
5. Only Jane can connect to the Real Audio server until the connection is closed or times out. The NBG420N times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

11.5.2 Two Points To Remember About Trigger Ports

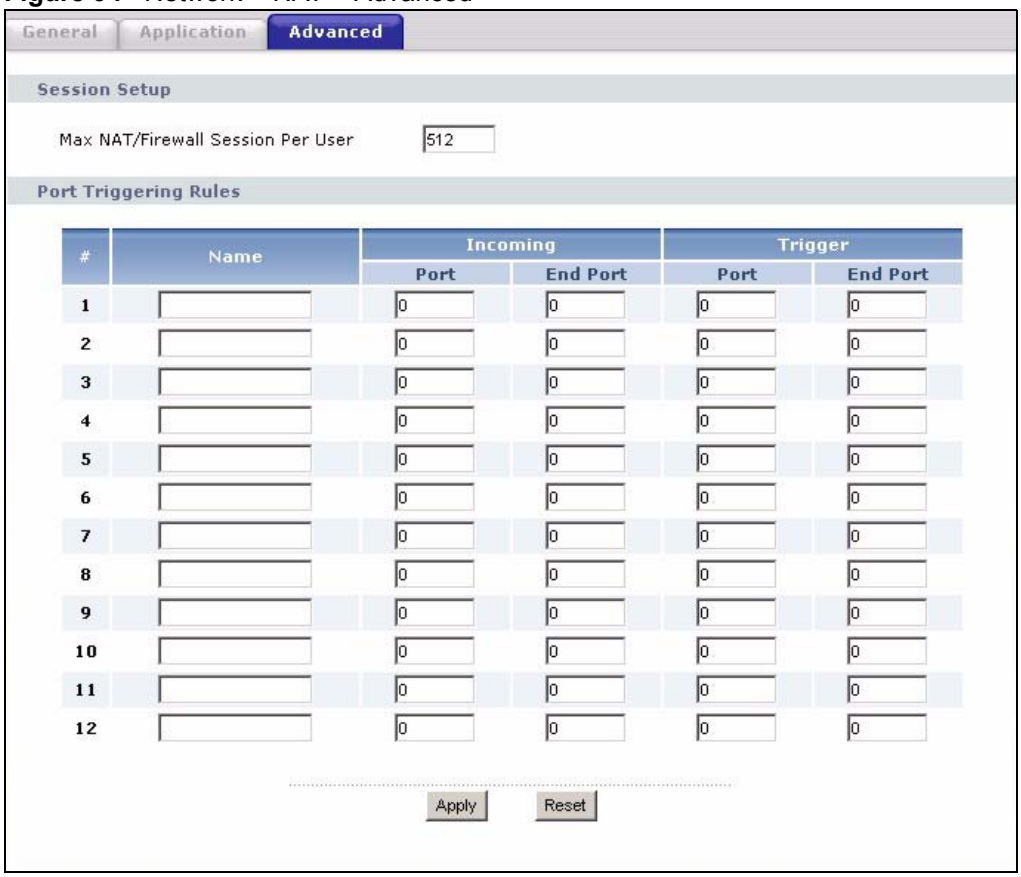
1. Trigger events only happen on data that is going coming from inside the NBG420N and going to the outside.
2. If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

11.6 NAT Advanced Screen

To change your NBG420N's trigger port settings, click **Network > NAT** > **Advanced**. The screen appears as shown.

Only one LAN computer can use a trigger port (range) at a time.

Figure 94 Network > NAT > Advanced



The following table describes the labels in this screen.

Table 55 Network > NAT > Advanced

LABEL	DESCRIPTION
Max NAT/Firewall Session Per User	Type a number ranging from 1 to 2048 to limit the number of NAT/firewall sessions that a host can create. When computers use peer to peer applications, such as file sharing applications, they may use a large number of NAT sessions. If you do not limit the number of NAT sessions a single client can establish, this can result in all of the available NAT sessions being used. In this case, no additional NAT sessions can be established, and users may not be able to access the Internet. Each NAT session establishes a corresponding firewall session. Use this field to limit the number of NAT/firewall sessions each client computer can establish through the NBG420N. If your network has a small number of clients using peer to peer applications, you can raise this number to ensure that their performance is not degraded by the number of NAT sessions they can establish. If your network has a large number of users using peer to peer applications, you can lower this number to ensure no single client is using all of the available NAT sessions.
Port Triggering Rules	
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.

Table 55 Network > NAT > Advanced

LABEL	DESCRIPTION
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The NBG420N forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the NBG420N to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

12

Dynamic DNS

12.1 Dynamic DNS Introduction

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

12.1.1 DynDNS Wildcard

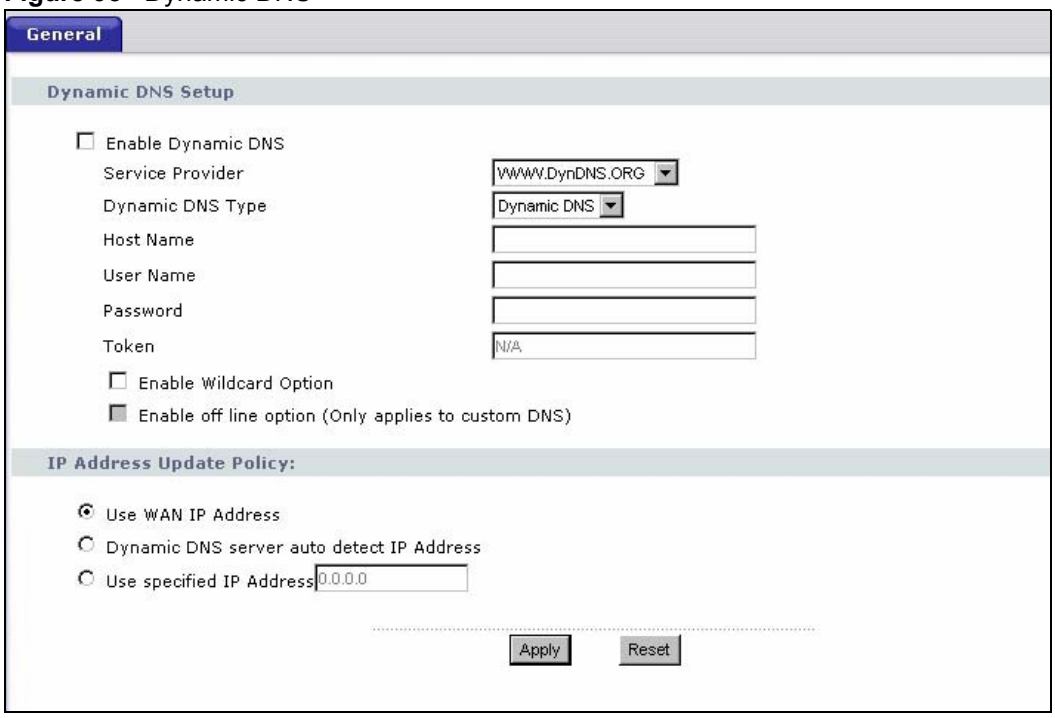
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

12.2 Dynamic DNS Screen

To change your NBG420N's DDNS, click **Network > DDNS**. The screen appears as shown.

Figure 95 Dynamic DNS



The following table describes the labels in this screen.

Table 56 Dynamic DNS

LABEL	DESCRIPTION
Enable Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Enter a host names in the field provided. You can specify up to two host names in the field separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Token	Enter your client authorization key provided by the server to update DynDNS records. This field is configurable only when you select **WWW.REGFISH.COM** in the **Service Provider** field.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option	This option is available when **CustomDNS** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy:	
Use WAN IP Address	Select this option to update the IP address of the host name(s) to the WAN IP address.
Dynamic DNS server auto detect IP Address	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.
Use specified IP Address	Type the IP address of the host name(s). Use this if you have a static IP address.

Table 56 Dynamic DNS

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

PART III
Security

Firewall (153)
Content Filtering (161)
IPSec VPN (165)

13

Firewall

This chapter gives some background information on firewalls and explains how to get started with the NBG420N's firewall.

13.1 Introduction to ZyXEL's Firewall

13.1.1 What is a Firewall?

Originally, the term "firewall" referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from a network that is not trusted. Of course, firewalls cannot solve every security problem. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

13.1.2 Stateful Inspection Firewall

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

13.1.3 About the NBG420N Firewall

The NBG420N firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click the **General** tab under **Firewall** and then click the **Enable Firewall** check box). The NBG420N's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The NBG420N can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The NBG420N is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The NBG420N has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

13.1.4 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via web configurator.
2. Think about access control before you connect to the network in any way, including attaching a modem to the port.
3. Limit who can access your router.
4. Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

13.2 Triangle Routes

If an alternate gateway on the LAN has an IP address in the same subnet as the NBG420N's LAN IP address, return traffic may not go through the NBG420N. This is called an asymmetrical or "triangle" route. This causes the NBG420N to reset the connection, as the connection has not been acknowledged.

You can have the NBG420N permit the use of asymmetrical route topology on the network (not reset the connection).

Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the NBG420N. A better solution is to use IP alias to put the NBG420N and the backup gateway on separate subnets.

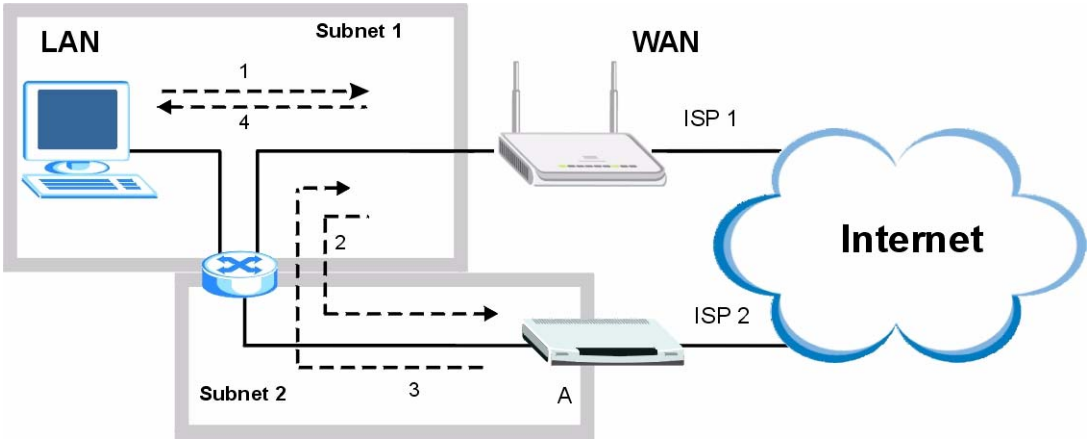
13.2.1 Triangle Routes and IP Alias

You can use IP alias instead of allowing triangle routes. IP Alias allow you to partition your network into logical sections over the same interface.

By putting your LAN and Gateway **A** in different subnets, all returning network traffic must pass through the NBG420N to your LAN. The following steps describe such a scenario.

1 A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
2 The NBG420N reroutes the packet to Gateway **A**, which is in **Subnet 2**.
3 The reply from the WAN goes to the NBG420N.
4 The NBG420N then sends it to the computer on the LAN in **Subnet 1**.

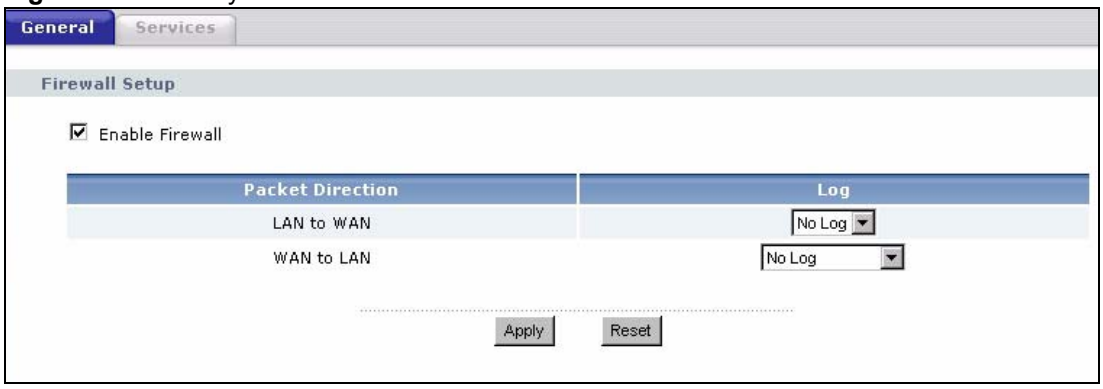
Figure 96 Using IP Alias to Solve the Triangle Route Problem



13.3 General Firewall Screen

Click **Security** > **Firewall** to open the **General** screen. Use this screen to enable or disable the NBG420N's firewall, and set up firewall logs.

Figure 97 Security > Firewall > General I



The following table describes the labels in this screen.

Table 57 Security > Firewall > General

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The NBG420N performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Packet Direction	This is the direction of travel of packets. Firewall rules are grouped based on the direction of travel of packets to which they apply.

Table 57 Security > Firewall > General

LABEL	DESCRIPTION
Log	Select whether to create a log for packets that are traveling in the selected direction when the packets are blocked (**Log All**) or forwarded (**Log Forward**). Or select **Not Log** to not log any records. To log packets related to firewall rules, make sure that **Access Control** under **Log** is selected in the **Logs** > **Log Settings** screen.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

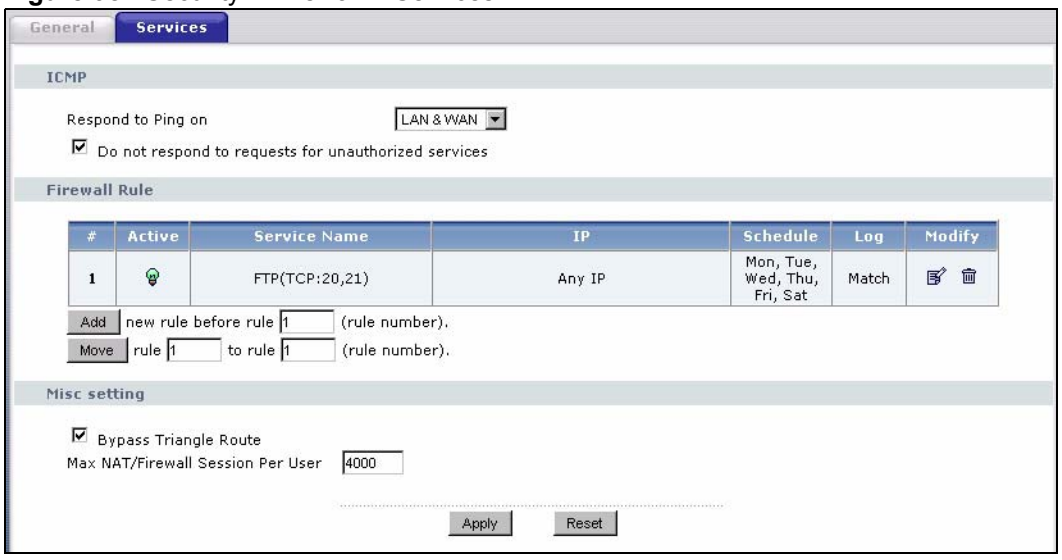
13.4 Services Screen

Click **Security** > **Firewall** > **Services**. The screen appears as shown next.

If an outside user attempts to probe an unsupported port on your NBG420N, an ICMP response packet is automatically returned. This allows the outside user to know the NBG420N exists. Use this screen to prevent the ICMP response packet from being sent. This keeps outsiders from discovering your NBG420N when unsupported ports are probed.

You can also use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

Figure 98 Security > Firewall > Services


General
Services
ICMP
Respond to Ping on
LAN & WAN
Do not respond to requests for unauthorized services
Firewall Rule
Active Service Name IP Schedule Log Modify
1 FTP(TCP:20,21) Any IP Mon, Tue, Wed, Thu, Fri, Sat Match
Add new rule before rule 1 (rule number).
Move rule 1 to rule 1 (rule number).
Misc setting
Bypass Triangle Route
Max NAT/Firewall Session Per User 4000
Apply
Reset

The following table describes the labels in this screen.

Table 58 Security > Firewall > Services

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The NBG420N will not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Otherwise select **LAN & WAN** to reply to all incoming LAN and WAN Ping requests.

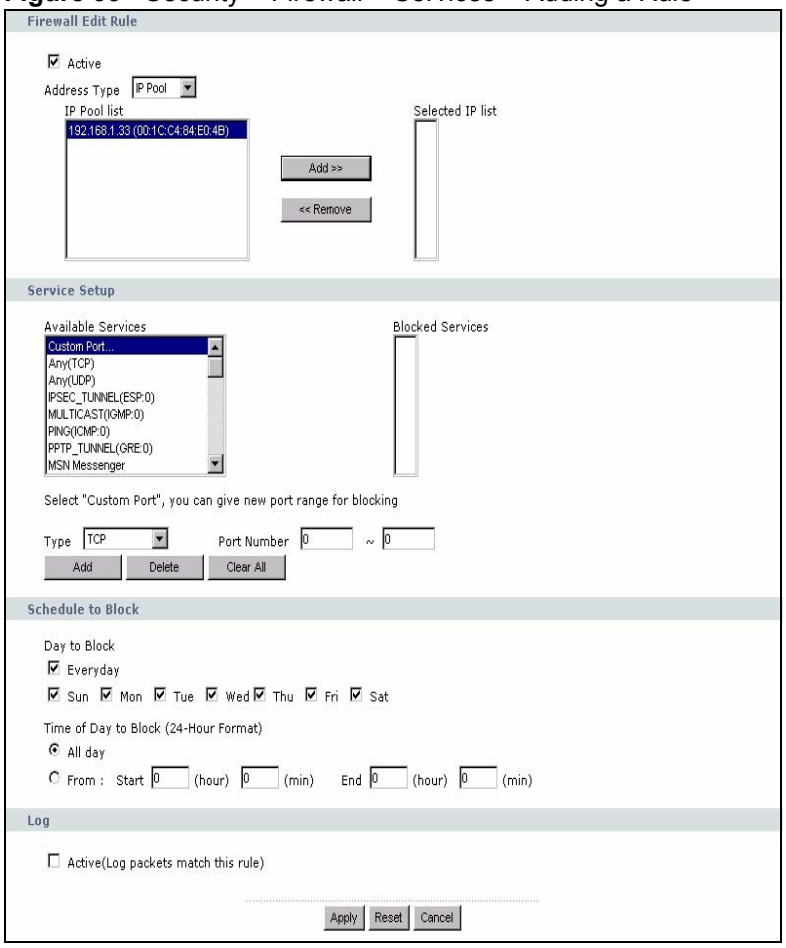
Table 58 Security > Firewall > Services

LABEL	DESCRIPTION
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the NBG420N by probing for unused ports. If you select this option, the NBG420N will not respond to port request(s) for unused ports, thus leaving the unused ports and the NBG420N unseen. By default this option is not selected and the NBG420N will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the NBG420N's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the NBG420N reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcprst rst [on|off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. Use the **Move** button to rearrange the order of the rules.
Active	This icon is green when the rule is turned on. The icon is grey when the rule is turned off.
Service Name	This field displays the services and port numbers to which this firewall rule applies.
IP	This field displays the IP address(es) the rule applies to.
Schedule	This field displays the days the firewall rule is active.
Log	This field shows you whether a log will be created when packets match the rule (**Match**) or not (**No**).
Modify	Click the **Edit** icon to modify an existing rule setting in the fields under the **Add Firewall Rule** screen. Click the **Remove** icon to delete a rule. Note that subsequent firewall rules move up by one when you take this action.
Add	Click the **Add** button to display the screen where you can configure a new firewall rule. Modify the number in the textbox to add the rule before a specific rule number.
Move	The **Move** button moves a rule to a different position. In the first text box enter the number of the rule you wish to move. In the second text box enter the number of the rule you wish to move the first rule to and click the **Move** button.
Misc setting	
Bypass Triangle Route	Select this check box to have the NBG420N firewall ignore the use of triangle route topology on the network.
Max NAT/Firewall Session Per User	Type a number ranging from 1 to 2048 to limit the number of NAT/firewall sessions that a host can create.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.

13.4.1 The Add Firewall Rule Screen

If you click Add or the Modify icon on an existing rule, the Add Firewall Rule screen is displayed. Use this screen to add a firewall rule or to modify an existing one.

Figure 99 Security > Firewall > Services > Adding a Rule



The following table describes the labels in this screen.

Table 59 Security > Firewall > Services > Adding a Rule

LABEL	DESCRIPTION
Active	Select this check box to turn the rule on.
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50), a pool of IP address or any IP address? Select an option from the drop-down list box that includes: **Any IP**, **Single IP**, **IP Range** and **IP Pool**.
IP Address	Enter the single IP address here. This field is only available when **Single IP** is selected as the **Address Type**.
Start IP Address	Enter the starting IP address in a range here. This field is only available when **IP Range** is selected as the **Address Type**.
End IP Address	Enter the ending IP address in a range here. This field is only available when **IP Range** is selected as the **Address Type**.
IP Pool List	Add an IP address from the **IP Pool List** to the **Selected IP List** by highlighting an IP address and clicking **Add**. To delete an IP address from the Selected IP List highlight an IP address and click the **Remove** button. These fields are only available when **IP Pool** is selected as the **Address Type**. The IP Pool list gathers its IPs from entries in the ARP table. The ARP table contains the IP addresses and MAC addresses of the devices that have sent traffic to the NBG420N.
Service Setup	

Table 59 Security > Firewall > Services > Adding a Rule

LABEL	DESCRIPTION
Available Services	This is a list of pre-defined services (ports) you may prohibit your LAN computers from using. Select the port you want to block using the drop-down list and click **Add** to add the port to the **Blocked Services** field.
Blocked Services	This is a list of services (ports) that will be inaccessible to computers on your LAN once you enable service blocking.
Custom Port	A custom port is a service that is not available in the pre-defined **Available Services** list and you must define using the next two fields.
Type	Choose the IP port (**TCP** or **UDP**) that defines your customized port from the drop down list box.
Port Number	Enter the port number range that defines the service. For example, if you want to define the Gnutella service, then select **TCP** type and enter a port range from 6345 to 6349.
Add	Select a service from the **Available Services** drop-down list and then click **Add** to add a service to the **Blocked Services**
Delete	Select a service from the **Blocked Services** list and then click **Delete** to remove this service from the list.
Clear All	Click **Clear All** to empty the **Blocked Services**.
Schedule to Block	
Day to Block:	Select a check box to configure which days of the week (or everyday) you want service blocking to be active.
Time of Day to Block (24-Hour Format)	Select the time of day you want service blocking to take effect. Configure blocking to take effect all day by selecting **All Day**. You can also configure specific times by selecting **From** and entering the start time in the **Start (hour)** and **Start (min)** fields and the end time in the **End (hour)** and **End (min)** fields. Enter times in 24-hour format, for example, "3:00pm" should be entered as "15:00".
Log	
Active (Log packets match this rule)	Select this to log packets that match this rule. Go to the **Log Settings** page and select the **Access Control** logs category to have the NBG420N record these logs.
Misc setting	
Bypass Triangle Route	Select this check box to have the NBG420N firewall ignore the use of triangle route topology on the network.
Max NAT/Firewall Session Per User	Type a number ranging from 1 to 2048 to limit the number of NAT/firewall sessions that a host can create.
Apply	Click **Apply** to save the settings.
Reset	Click **Reset** to start configuring this screen again.
Cancel	Click **Cancel** to return to the **Services** screen without saving any changes.

14

Content Filtering

This chapter provides a brief overview of content filtering using the embedded web GUI.

14.1 Introduction to Content Filtering

Internet content filtering allows you to create and enforce Internet access policies tailored to your needs. Content filtering is the ability to block certain web features or specific URL keywords.

14.2 Restrict Web Features

The NBG420N can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.

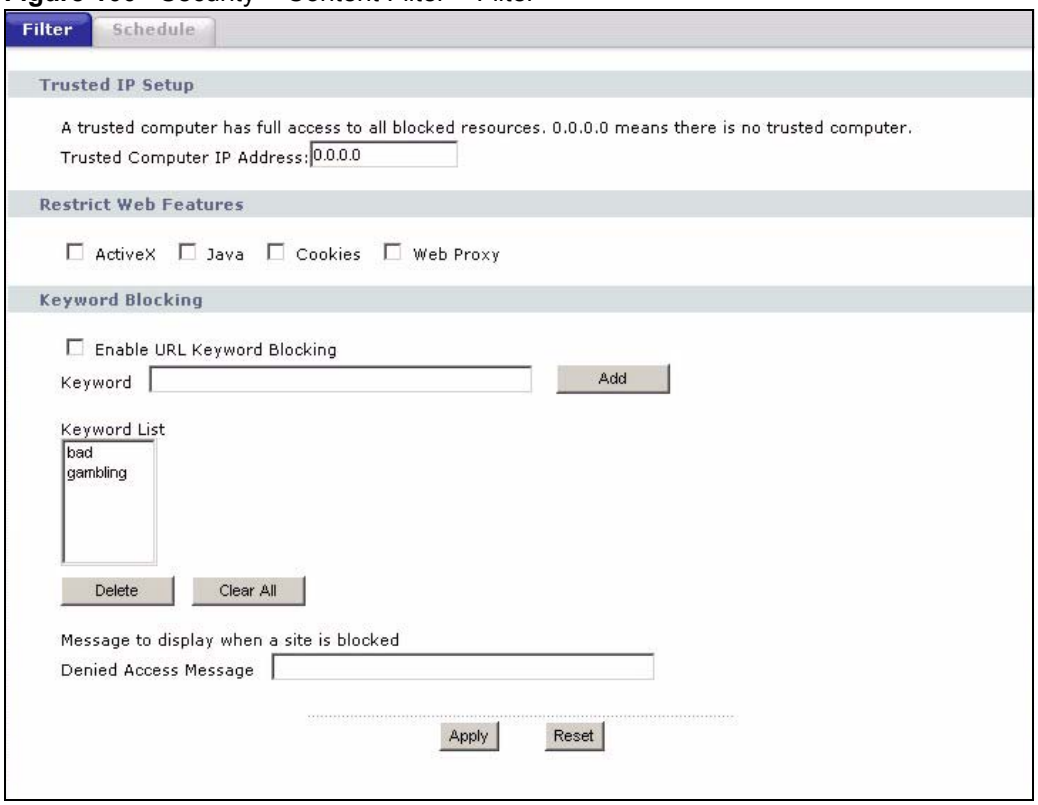
14.3 Days and Times

The NBG420N also allows you to define time periods and days during which the NBG420N performs content filtering.

14.4 Filter Screen

Click **Security** > **Content Filter** to open the **Filter** screen.

Figure 100 Security > Content Filter > Filter



The following table describes the labels in this screen.

Table 60 Security > Content Filter > Filter

LABEL	DESCRIPTION
Trusted Computer IP Address	To enable this feature, type an IP address of any one of the computers in your network that you want to have as a trusted computer. This allows the trusted computer to have full access to all features that are configured to be blocked by content filtering. Leave this field blank to have no trusted computers.
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Keyword Blocking	
Enable URL Keyword Blocking	The NBG420N can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL http://www.website.com/bad.html would be blocked. Select this check box to enable this feature.

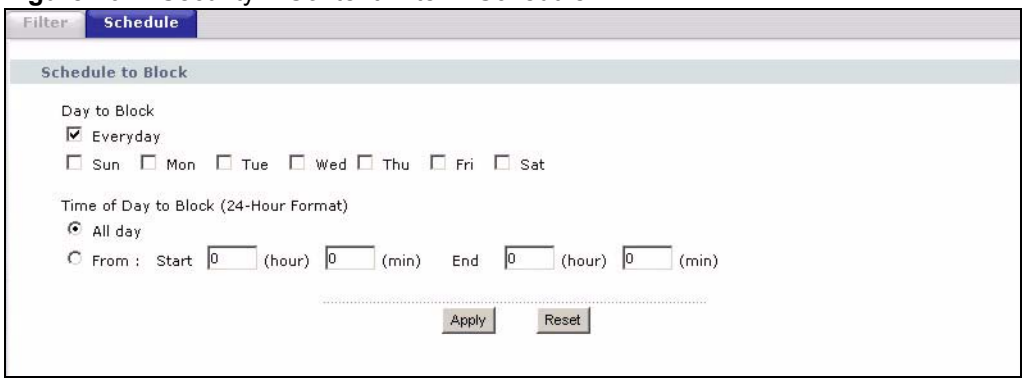
Table 60 Security > Content Filter > Filter

LABEL	DESCRIPTION
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.
Add	Click **Add** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click **Delete** to remove it. The keyword disappears from the text box after you click **Apply**.
Clear All	Click this button to remove all of the listed keywords.
Denied Access Message	Enter a message to be displayed when a user tries to access a restricted web site. The default message is “Please contact your network administrator!!”
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh

14.5 Schedule

Use this screen to set the day(s) and time you want the NBG420N to use content filtering. Click **Security** > **Content Filter** > **Schedule**. The following screen displays.

Figure 101 Security > Content Filter > Schedule



The following table describes the labels in this screen.

Table 61 Security > Content Filter > Schedule

LABEL	DESCRIPTION
Day to Block	Select check boxes for the days that you want the NBG420N to perform content filtering. Select the **Everyday** check box to have content filtering turned on all days of the week.
Time of Day to Block (24-Hour Format)	**Time of Day to Block** allows the administrator to define during which time periods content filtering is enabled. **Time of Day to Block** restrictions only apply to the keywords (see above). Restrict web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected. Select **All Day** to have content filtering always active on the days selected in **Day to Block** with time of day limitations not enforced. Select **From** and enter the time period, in 24-hour format, during which content filtering will be enforced.

Table 61 Security > Content Filter > Schedule

LABEL	DESCRIPTION
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh

14.6 Customizing Keyword Blocking URL Checking

You can use commands to set how much of a website's URL the content filter is to check for keyword blocking. See the appendices for information on how to access and use the command interpreter.

14.6.1 Domain Name or IP Address URL Checking

By default, the NBG420N checks the URL's domain name or IP address when performing keyword blocking.

This means that the NBG420N checks the characters that come before the first slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, content filtering only searches for keywords within www.zyxel.com.tw.

14.6.2 Full Path URL Checking

Full path URL checking has the NBG420N check the characters that come before the last slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, full path URL checking searches for keywords within www.zyxel.com.tw/news/.

Use the `ip urlfilter customize actionFlags 6 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's full path.

14.6.3 File Name URL Checking

Filename URL checking has the NBG420N check all of the characters in the URL.

For example, filename URL checking searches for keywords within the URL www.zyxel.com.tw/news/pressroom.php.

Use the `ip urlfilter customize actionFlags 8 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's complete filename.

15 IPSec VPN

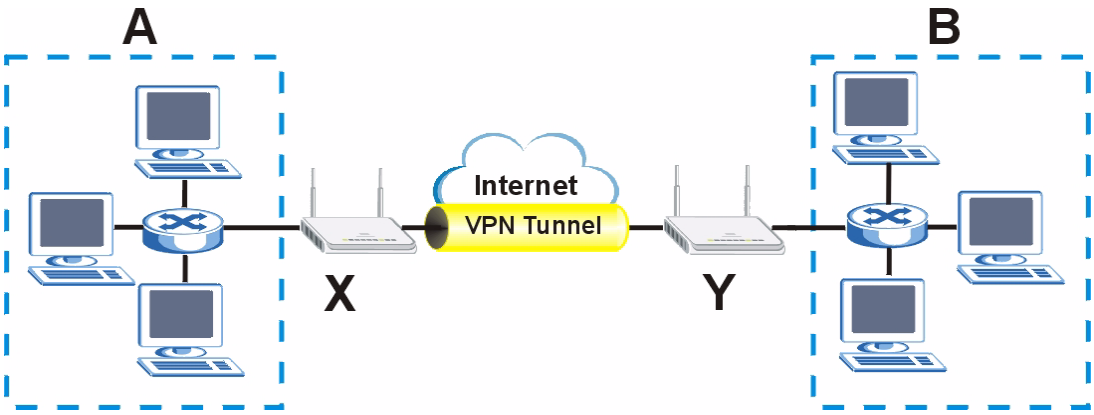
15.1 IPSec VPN Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

The following figure provides one perspective of a VPN tunnel.

Figure 102 IPSec VPN: Overview



The VPN tunnel connects the NBG420N (**X**) and the remote IPSec router (**Y**). These routers then connect the local network (**A**) and remote network (**B**).

15.1.1 What You Can Do in the IPSec VPN Screens

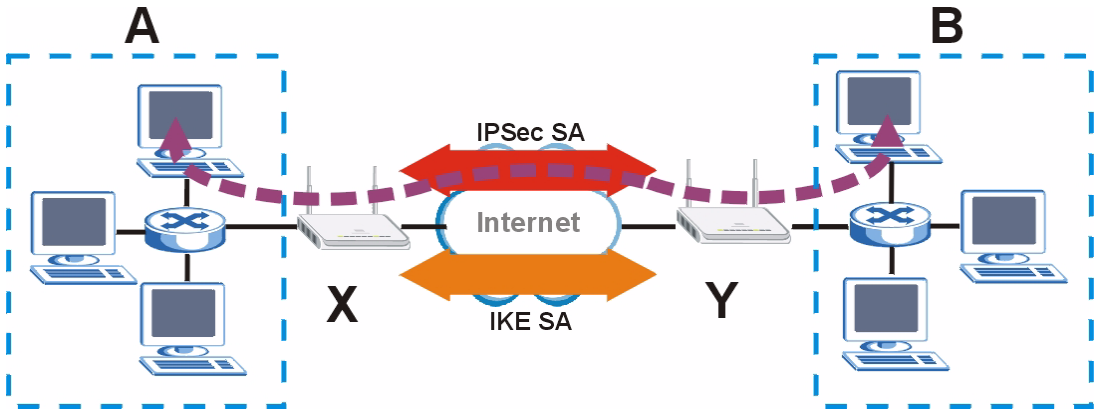
Use the **General** Screen (Section 15.2 on page 167) to display and manage the NBG420N's VPN rules (tunnels).

Use the **SA Monitor** Screen (Section 15.3 on page 183) to display and manage active VPN connections.

15.1.2 What You Need To Know About IPSec VPN

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the NBG420N and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the NBG420N and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the NBG420N and remote IPSec router can send data between computers on the local network and remote network. The following figure illustrates this.

Figure 103 VPN: IKE SA and IPSec SA



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is established securely using the IKE SA that routers **X** and **Y** established first.

15.1.3 IKE SA (IKE Phase 1) Overview

The IKE SA provides a secure connection between the NBG420N and remote IPSec router.

It takes several steps to establish an IKE SA. The negotiation mode determines the number of steps to use. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Note: Both routers must use the same negotiation mode.

These modes are discussed in more detail in Negotiation Mode on page 187. Main mode is used in various examples in the rest of this section.

15.1.3.1 IP Addresses of the NBG420N and Remote IPSec Router

In the NBG420N, you have to specify the IP addresses of the NBG420N and the remote IPSec router to establish an IKE SA.

You can usually provide a static IP address or a domain name for the NBG420N. Sometimes, your NBG420N might also offer another alternative, such as using the IP address of a port or interface.

You can usually provide a static IP address or a domain name for the remote IPSec router as well. Sometimes, you might not know the IP address of the remote IPSec router (for example, telecommuters). In this case, you can still set up the IKE SA, but only the remote IPSec router can initiate an IKE SA.

15.1.4 IPSec SA (IKE Phase 2) Overview

Once the NBG420N and remote IPSec router have established the IKE SA, they can securely negotiate an IPSec SA through which to send data between computers on the networks.

Note: The IPSec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of an IPSec SA.

15.1.4.1 Local Network and Remote Network

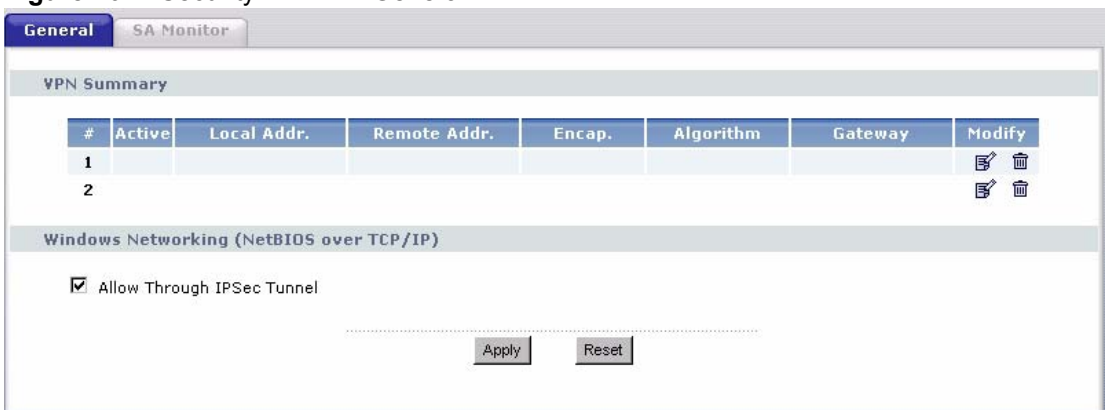
In an IPSec SA, the local network consists of devices connected to the NBG420N and may be called the local policy. Similarly, the remote network consists of the devices connected to the remote IPSec router and may be called the remote policy.

Note: It is not recommended to set a VPN rule's local and remote network settings both to 0.0.0.0 (any). This causes the NBG420N to try to forward all access attempts (to the local network, the Internet or even the NBG420N) to the remote IPSec router. In this case, you can no longer manage the NBG420N.

15.2 The General Screen

Click **Security > VPN** to display the **Summary** screen. This is a read-only menu of your VPN rules (tunnels). Edit a VPN rule by clicking the **Edit** icon.

Figure 104 Security > VPN > General



The following table describes the fields in this screen.

Table 62 Security > VPN > General

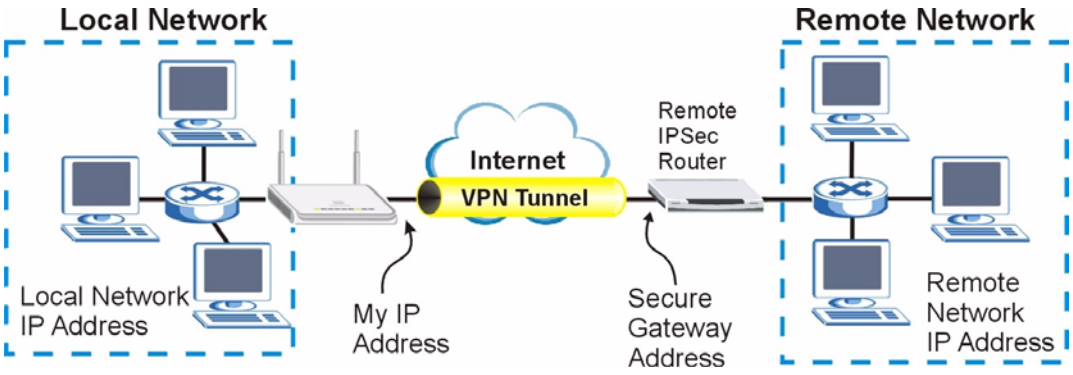
LABEL	DESCRIPTION
#	This is the VPN policy index number.
Active	This field displays whether the VPN policy is active or not. This icon is turned on when the rule is enabled.
Local Addr.	This displays the beginning and ending (static) IP addresses or a (static) IP address and a subnet mask of computer(s) on your local network behind your NBG420N.
Remote Addr.	This displays the beginning and ending (static) IP addresses or a (static) IP address and a subnet mask of computer(s) on the remote network behind the remote IPSec router. This field displays **0.0.0.0** when the **Secure Gateway Address** field displays **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN.
Encap.	This field displays **Tunnel** or **Transport** mode (**Tunnel** is the default selection).
Algorithm	This field displays the security protocol, encryption algorithm and authentication algorithm used for an SA.
Gateway	This is the static WAN IP address or URL of the remote IPSec router. This field displays **0.0.0.0** when you configure the **Secure Gateway Address** field in the **Rule Setup** screen to **0.0.0.0.**
Modify	Click the **Edit** icon to go to the screen where you can edit the VPN rule. Click the **Remove** icon to remove an existing VPN rule.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.
Allow NetBIOS Traffic Through IPSec Tunnel	Select this check box to send NetBIOS packets through the VPN connection.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

15.2.1 VPN Rule Setup (Basic)

Click the **Edit** icon in the **General** screen to display the **Rule Setup** screen.

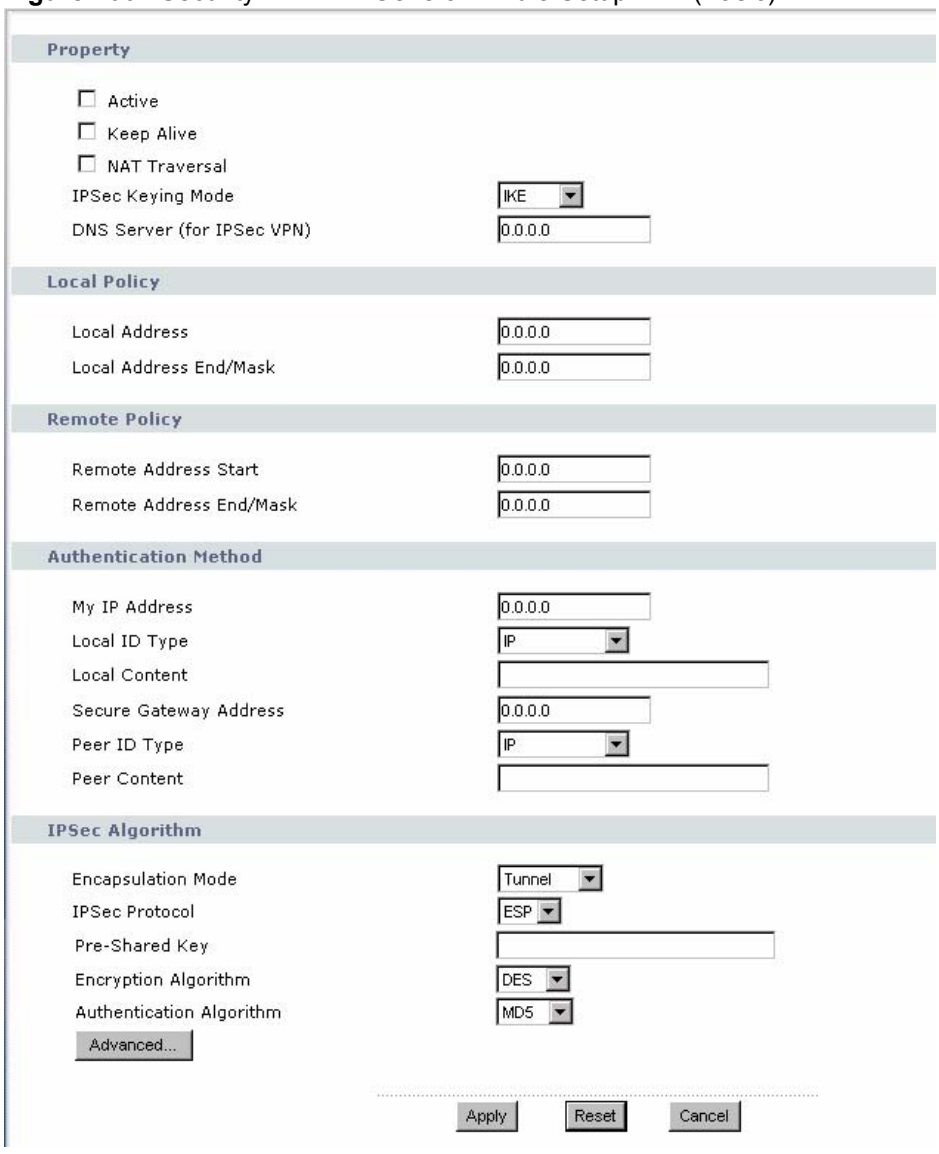
This figure helps explain the main fields.

Figure 105 IPSec Fields Summary



Use this screen to configure a VPN rule.

Figure 106 Security > VPN > General > Rule Setup: IKE (Basic)



The following table describes the labels in this screen.

Table 63 SECURITY > VPN > Rule Setup: IKE (Basic)

LABEL	DESCRIPTION
Property	
Active	Select this check box to activate this VPN policy.
Keep Alive	Select this check box to have the NBG420N automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
NAT Traversal	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers. **Note:** The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP ports 500 and 4500 to the IPSec router behind the NAT router.
IPSec Keying Mode	Select **IKE** or **Manual** from the drop-down list box. **IKE** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The NBG420N assigns this additional DNS server to the NBG420N's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local Policy	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
Local Address	For a single IP address, enter a (static) IP address on the LAN behind your NBG420N. For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on your LAN behind your NBG420N. To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the LAN behind your NBG420N.
Local Address End /Mask	When the local IP address is a single address, type it a second time here. When the local IP address is a range, enter the end (static) IP address, in a range of computers on the LAN behind your NBG420N. When the local IP address is a subnet address, enter a subnet mask on the LAN behind your NBG420N.

Table 63 SECURITY > VPN > Rule Setup: IKE (Basic) (continued)

LABEL	DESCRIPTION
Remote Policy	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the **Secure Gateway IP Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address	For a single IP address, enter a (static) IP address on the network behind the remote IPSec router. For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the network behind the remote IPSec router.
Remote Address End /Mask	When the remote IP address is a single address, type it a second time here. When the remote IP address is a range, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the remote IP address is a subnet address, enter a subnet mask on the network behind the remote IPSec router.
Authentication Method	
My IP Address	Enter the NBG420N's static WAN IP address (if it has one) or leave the field set to **0.0.0.0**. The NBG420N uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. If the WAN connection goes down, the NBG420N uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. Otherwise, you can enter one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the NBG420N use that dynamic domain name's IP address. The VPN tunnel has to be rebuilt if **My IP Address** changes after setup.
Local ID Type	Select **IP** to identify this NBG420N by its IP address. Select **Domain Name** to identify this NBG420N by a domain name. Select **E-mail** to identify this NBG420N by an e-mail address.
Local Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the **Local Content** field. The NBG420N automatically uses the IP address in the **My IP Address** field (refer to the **My IP Address** field description) if you configure the **Local Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the **Local Content** field or use the **Domain Name** or **E-mail** ID type in the following situations. • When there is a NAT router between the two IPSec routers. • When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **Domain Name** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this NBG420N in the **Local Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.

Table 63 SECURITY > VPN > Rule Setup: IKE (Basic) (continued)

LABEL	DESCRIPTION
Secure Gateway Address	Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address (the **IPSec Keying Mode** field must be set to **IKE**). In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**. **Note:** You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The NBG420N has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **Domain Name** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Peer Content	The configuration of the peer content depends on the peer ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the NBG420N will use the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description). For **Domain Name** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than **0.0.0.0** or use the **Domain Name** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the NBG420N to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.
IPSec Algorithm	
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
IPSec Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase processing requirements and communications latency (delay). If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below).

Table 63 SECURITY > VPN > Rule Setup: IKE (Basic) (continued)

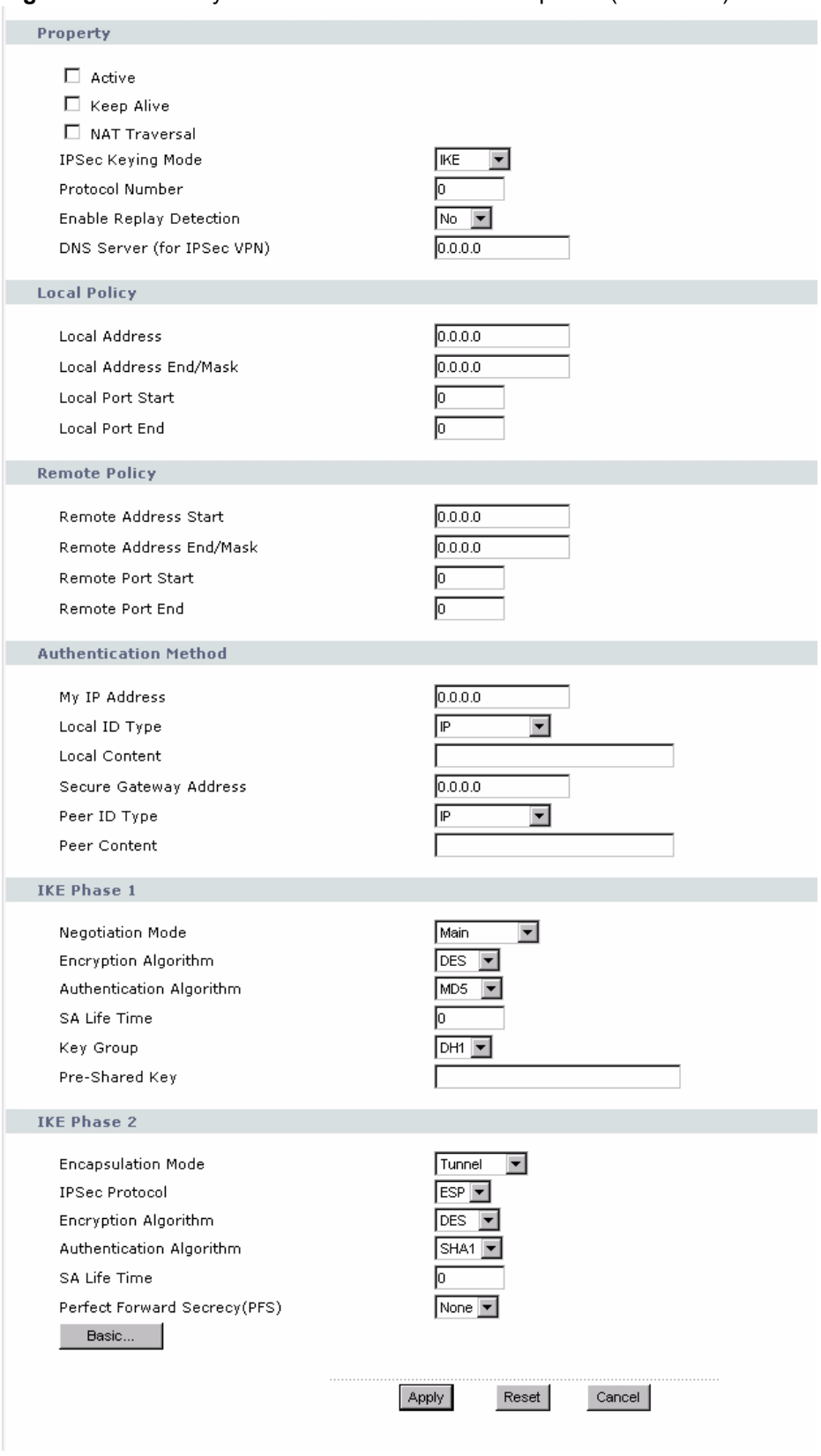
LABEL	DESCRIPTION
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a “PYLD_MALFORMED” (payload malformed) packet if the same pre-shared key is not used on both ends.
Encryption Algorithm	Select which key size and encryption algorithm to use for data communications. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm The NBG420N and the remote IPSec router must use the same algorithms and key , which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
Advanced...	Click **Advanced...** to configure more detailed settings of your IKE key management.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.
Cancel	Click **Cancel** to exit the screen without making any changes.

15.2.2 VPN Rule Setup (Advanced)

Click the **Advanced...** button in the **Rule Setup** screen to open this screen.

Use this screen to configure a VPN rule.

Figure 107 Security > VPN > General > Rule Setup: IKE (Advanced)



The following table describes the labels in this screen.

Table 64 Security > VPN > Rule Setup: IKE (Advanced)

LABEL	DESCRIPTION
Property	
Active	Select this check box to activate this VPN policy.
Keep Alive	Select this check box to have the NBG420N automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
NAT Traversal	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers. **Note:** The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP ports 500 and 4500 to the IPSec router behind the NAT router.
IPSec Keying Mode	Select **IKE** or **Manual** from the drop-down list box. **IKE** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
Protocol Number	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Select **Yes** from the drop-down menu to enable replay detection, or select **No** to disable it.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The NBG420N assigns this additional DNS server to the NBG420N's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local Policy	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
Local Address	For a single IP address, enter a (static) IP address on the LAN behind your NBG420N. For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on your LAN behind your NBG420N. To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the LAN behind your NBG420N.

Table 64 Security > VPN > Rule Setup: IKE (Advanced) (continued)

LABEL	DESCRIPTION
Local Address End / Mask	When the local IP address is a single address, type it a second time here. When the local IP address is a range, enter the end (static) IP address, in a range of computers on the LAN behind your NBG420N. When the local IP address is a subnet address, enter a subnet mask on the LAN behind your NBG420N.
Local Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Local Port End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Local Port Start** is left at 0, **Local Port End** will also remain at 0.
Remote Policy	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the **Secure Gateway IP Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address	For a single IP address, enter a (static) IP address on the network behind the remote IPSec router. For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the network behind the remote IPSec router.
Remote Address End /Mask	When the remote IP address is a single address, type it a second time here. When the remote IP address is a range, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the remote IP address is a subnet address, enter a subnet mask on the network behind the remote IPSec router.
Remote Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Remote Port End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Remote Port Start** is left at 0, **Remote Port End** will also remain at 0.
Authentication Method	
My IP Address	Enter the NBG420N's static WAN IP address (if it has one) or leave the field set to **0.0.0.0**. The NBG420N uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. If the WAN connection goes down, the NBG420N uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. Otherwise, you can enter one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the NBG420N use that dynamic domain name's IP address. The VPN tunnel has to be rebuilt if **My IP Address** changes after setup.
Local ID Type	Select **IP** to identify this NBG420N by its IP address. Select **Domain Name** to identify this NBG420N by a domain name. Select **E-mail** to identify this NBG420N by an e-mail address.

Table 64 Security > VPN > Rule Setup: IKE (Advanced) (continued)

LABEL	DESCRIPTION
Local Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the **Local Content** field. The NBG420N automatically uses the IP address in the **My IP Address** field (refer to the **My IP Address** field description) if you configure the **Local Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the **Local Content** field or use the **Domain Name** or **E-mail** ID type in the following situations. • When there is a NAT router between the two IPSec routers. • When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **Domain Name** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this NBG420N in the **Local Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Secure Gateway Address	Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address (the **IPSec Keying Mode** field must be set to **IKE**). In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**. **Note:** You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The NBG420N has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **Domain Name** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Peer Content	The configuration of the peer content depends on the peer ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the NBG420N will use the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description). For **Domain Name** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than **0.0.0.0** or use the **Domain Name** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the NBG420N to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.

Table 64 Security > VPN > Rule Setup: IKE (Advanced) (continued)

LABEL	DESCRIPTION
IKE Phase 1	
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm The NBG420N and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data in the IKE SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 180 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	Select which Diffie-Hellman key group (DH*x*) you want to use for encryption keys. Choices are: **DH1** - use a 768-bit random number **DH2** - use a 1024-bit random number
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a “PYLD_MALFORMED” (payload malformed) packet if the same pre-shared key is not used on both ends.
IKE Phase 2	
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode.
IPSec Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase processing requirements and communications latency (delay). If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below).
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm The NBG420N and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.

Table 64 Security > VPN > Rule Setup: IKE (Advanced) (continued)

LABEL	DESCRIPTION
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
SA Life Time	Define the length of time before an IPSec SA automatically renegotiates in this field. The minimum value is 180 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secrecy (PFS)	Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are: **None** - disable PFS **DH1** - enable PFS and use a 768-bit random number **DH2** - enable PFS and use a 1024-bit random number PFS changes the root key that is used to generate encryption keys for each IPSec SA. It is more secure but takes more time.
Basic...	Click **Basic...** to go to the previous VPN configuration screen.
Apply	Click **Apply** to save the changes.
Reset	Click **Reset** to begin configuring this screen afresh.
Cancel	Click **Cancel** to exit the screen without making any changes.

15.2.3 VPN Rule Setup (Manual)

Use this screen to configure VPN rules (tunnels) that use manual keys. Manual key management is useful if you have problems with IKE key management.

Select **Manual** in the **IPSec Keying Mode** field on the **Rule Setup** screen to open the screen as shown in Figure 108 on page 180.

15.2.3.1 IPSec SA Using Manual Keys

You might set up an IPSec SA using manual keys when you want to establish a VPN tunnel quickly, for example, for troubleshooting. You should only do this as a temporary solution, however, because it is not as secure as a regular IPSec SA.

In IPSec SAs using manual keys, the NBG420N and remote IPSec router do not establish an IKE SA. They only establish an IPSec SA. As a result, an IPSec SA using manual keys has some characteristics of IKE SA and some characteristics of IPSec SA. There are also some differences between IPSec SA using manual keys and other types of SA.

15.2.3.2 IPSec SA Proposal Using Manual Keys

In IPSec SA using manual keys, you can only specify one encryption algorithm and one authentication algorithm. There is no DH key exchange, so you have to provide the encryption key and the authentication key the NBG420N and remote IPSec router use.

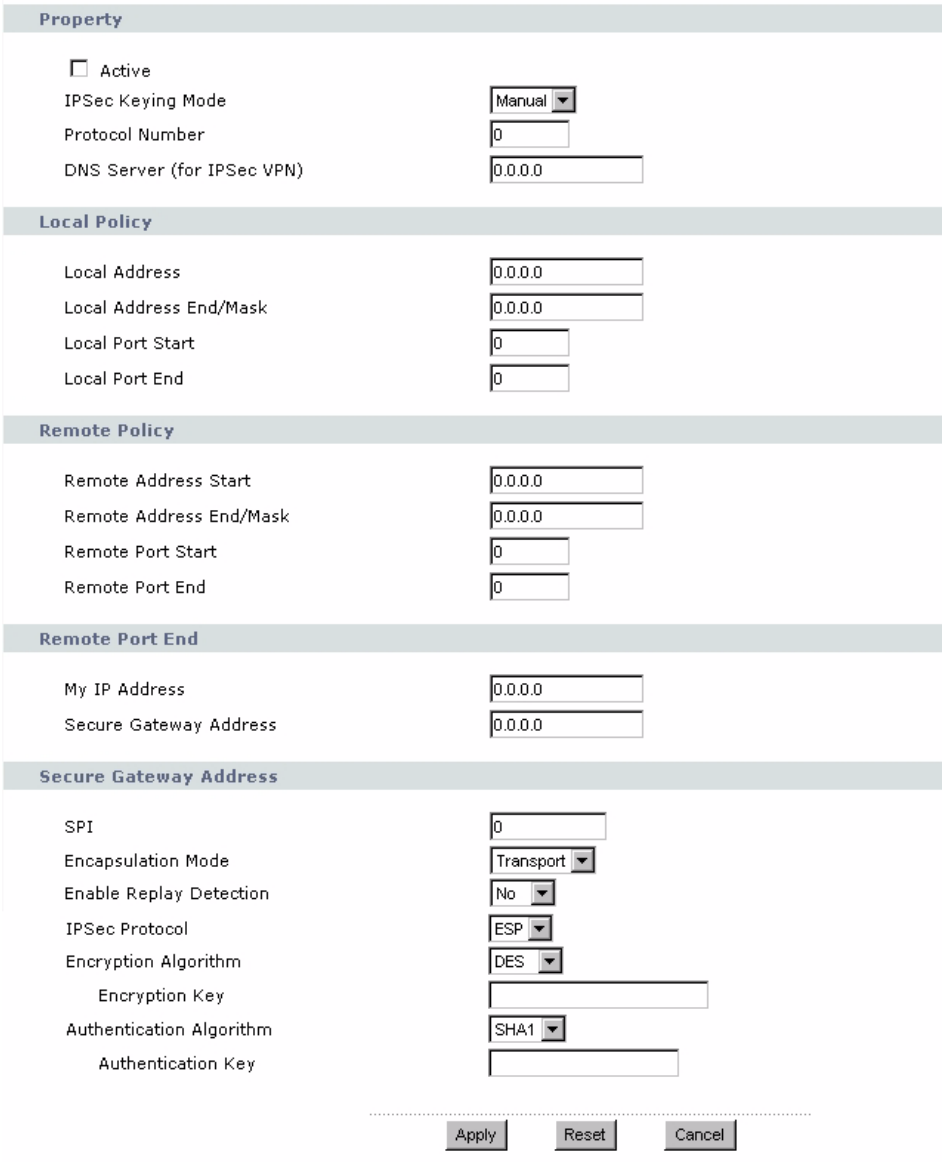
Note: The NBG420N and remote IPSec router must use the same encryption key and authentication key.

15.2.3.3 Authentication and the Security Parameter Index (SPI)

For authentication, the NBG420N and remote IPSec router use the SPI, instead of pre-shared keys, ID type and content. The SPI is an identification number.

Note: The NBG420N and remote IPSec router must use the same SPI.

Figure 108 Security > VPN > General > Rule Setup: Manual



The following table describes the labels in this screen.

Table 65 Security > VPN > Rule Setup: Manual

LABEL	DESCRIPTION
Property	
Active	Select this check box to activate this VPN policy.

Table 65 Security > VPN > Rule Setup: Manual (continued)

LABEL	DESCRIPTION
IPSec Keying Mode	Select **IKE** or **Manual** from the drop-down list box. **IKE** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
Protocol Number	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The NBG420N assigns this additional DNS server to the NBG420N's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local Policy	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
Local Address	For a single IP address, enter a (static) IP address on the LAN behind your NBG420N. For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on your LAN behind your NBG420N. To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the LAN behind your NBG420N.
Local Address End /Mask	When the local IP address is a single address, type it a second time here. When the local IP address is a range, enter the end (static) IP address, in a range of computers on the LAN behind your NBG420N. When the local IP address is a subnet address, enter a subnet mask on the LAN behind your NBG420N.
Local Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Local Port End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Local Port Start** is left at 0, **Local Port End** will also remain at 0.
Remote Policy	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the **Secure Gateway IP Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.

Table 65 Security > VPN > Rule Setup: Manual (continued)

LABEL	DESCRIPTION
Remote Address	For a single IP address, enter a (static) IP address on the network behind the remote IPSec router. For a specific range of IP addresses, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. To specify IP addresses on a network by their subnet mask, enter a (static) IP address on the network behind the remote IPSec router.
Remote Address End /Mask	When the remote IP address is a single address, type it a second time here. When the remote IP address is a range, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the remote IP address is a subnet address, enter a subnet mask on the network behind the remote IPSec router.
Remote Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Remote Port End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Remote Port Start** is left at 0, **Remote Port End** will also remain at 0.
My IP Address	Enter the NBG420N's static WAN IP address (if it has one) or leave the field set to **0.0.0.0**. The NBG420N uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. If the WAN connection goes down, the NBG420N uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. Otherwise, you can enter one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the NBG420N use that dynamic domain name's IP address. The VPN tunnel has to be rebuilt if **My IP Address** changes after setup.
Secure Gateway Address	Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address (the **IPSec Keying Mode** field must be set to **IKE**). In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**. **Note:** You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The NBG420N has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).
SPI	Type a unique **SPI** (Security Parameter Index) from one to four characters long. Valid Characters are "0, 1, 2, 3, 4, 5, 6, 7, 8, and 9".
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.

Table 65 Security > VPN > Rule Setup: Manual (continued)

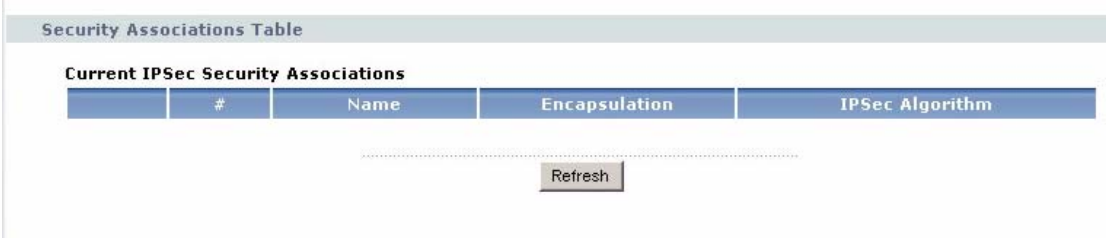
LABEL	DESCRIPTION
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Select **Yes** from the drop-down menu to enable replay detection, or select **No** to disable it.
IPSec Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase processing requirements and communications latency (delay). If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below).
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm The NBG420N and the remote IPSec router must use the same algorithms and keys. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Encryption Key	This field is applicable when you select **ESP** in the **IPSec Protocol** field above. With **DES**, type a unique key 8 characters long. With **3DES**, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA-1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.
Cancel	Click **Cancel** to exit the screen without making any changes.

15.3 The SA Monitor Screen

In the web configurator, click **Security > VPN > SA Monitor**. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections.

Figure 109 Security > VPN > SA Monitor



The following table describes the labels in this screen.

Table 66 Security > VPN > SA Monitor

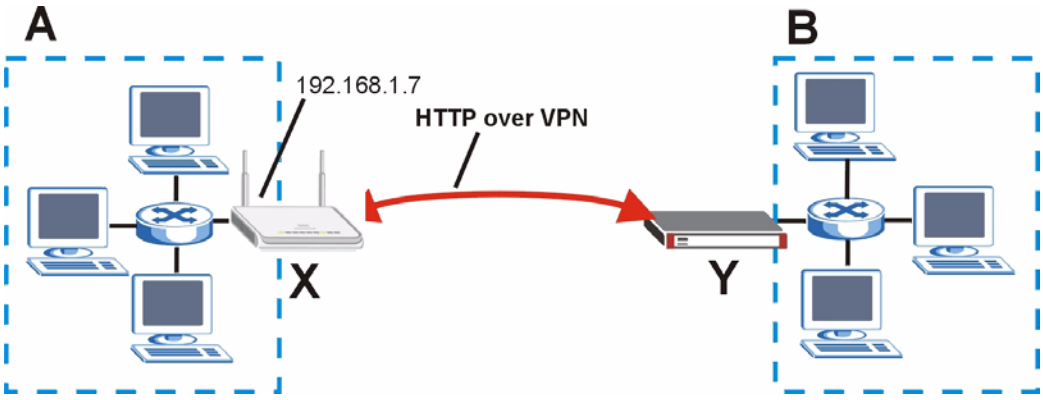
LABEL	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase NBG420N processing requirements and communications latency (delay).
Refresh	Click **Refresh** to display the current active VPN connection(s).

15.4 VPN and Remote Management

You can allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the NBG420N. One of the NBG420N's ports must be part of the VPN rule's local network. This can be the NBG420N's LAN port if you do not want to allow remote management on the WAN port. You also have to configure remote management (**REMOTE MGMT**) to allow management access for the service through the specific port.

In the following example, the VPN rule's local network (A) includes the NBG420N's LAN IP address of 192.168.1.7. Someone in the remote network (B) can use a service (like HTTP for example) through the VPN tunnel to access the NBG420N's LAN interface. Remote management must also be configured to allow HTTP access on the NBG420N's LAN interface.

Figure 110 VPN for Remote Management Example

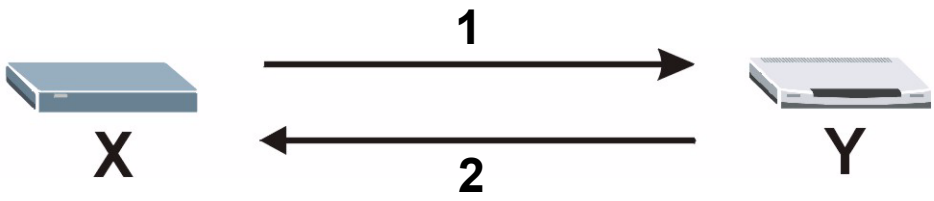


15.5 IPSec VPN Technical Reference

IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the NBG420N and remote IPSec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated below.

Figure 111 IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal



The NBG420N sends a proposal to the remote IPSec router. Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the NBG420N wants to use in the IKE SA. The remote IPSec router sends the accepted proposal back to the NBG420N. If the remote IPSec router rejects the proposal (for example, if the VPN tunnel is not configured correctly), the NBG420N and remote IPSec router cannot establish an IKE SA.

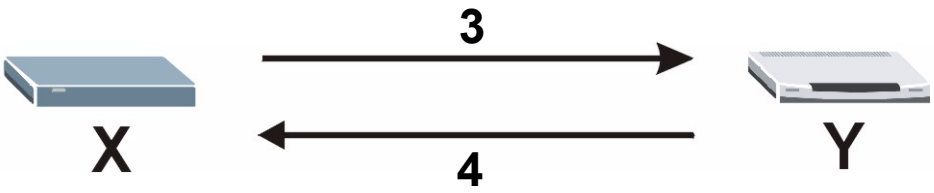
Note: Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

See the field descriptions for information about specific encryption algorithms, authentication algorithms, and DH key groups. See Diffie-Hellman (DH) Key Exchange on page 185 for more information about DH key groups.

Diffie-Hellman (DH) Key Exchange

The NBG420N and the remote IPSec router use a DH key exchange to establish a shared secret, which is used to generate encryption keys for IKE SA and IPSec SA. In main mode, the DH key exchange is done in steps 3 and 4, as illustrated below.

Figure 112 IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



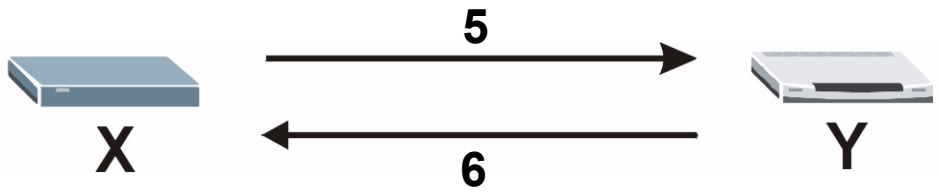
The DH key exchange is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption keys, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 encryption keys take longer to encrypt and decrypt.

Authentication

Before the NBG420N and remote IPSec router establish an IKE SA, they have to verify each other's identity. This process is based on pre-shared keys and router identities.

In main mode, the NBG420N and remote IPSec router authenticate each other in steps 5 and 6, as illustrated below. Their identities are encrypted using the encryption algorithm and encryption key the NBG420N and remote IPSec router selected in previous steps.

Figure 113 IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication



The NBG420N and remote IPSec router use a pre-shared key in the authentication process, though it is not actually transmitted or exchanged.

Note: The NBG420N and the remote IPSec router must use the same pre-shared key.

Router identity consists of ID type and ID content. The ID type can be IP address, domain name, or e-mail address, and the ID content is a specific IP address, domain name, or e-mail address. The ID content is only used for identification; the IP address, domain name, or e-mail address that you enter does not have to actually exist.

The NBG420N and the remote IPSec router each has its own identity, so each one must store two sets of information, one for itself and one for the other router. Local ID type and ID content refers to the ID type and ID content that applies to the router itself, and peer ID type and ID content refers to the ID type and ID content that applies to the other router in the IKE SA.

Note: The NBG420N's local and peer ID type and ID content must match the remote IPSec router's peer and local ID type and ID content, respectively.

In the following example, the ID type and content match so the NBG420N and the remote IPSec router authenticate each other successfully.

Table 67 VPN Example: Matching ID Type and Content

NBG420N	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

In the following example, the ID type and content do not match so the authentication fails and the NBG420N and the remote IPSec router cannot establish an IKE SA.

Table 68 VPN Example: Mismatching ID Type and Content

NBG420N	REMOTE IPSEC ROUTER
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.15	Peer ID content: tom@yourcompany.com

Negotiation Mode

There are two negotiation modes: main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1-2: The NBG420N sends its proposals to the remote IPSec router. The remote IPSec router selects an acceptable proposal and sends it back to the NBG420N.

Steps 3-4: The NBG420N and the remote IPSec router participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

Steps 5-6: Finally, the NBG420N and the remote IPSec router generate an encryption key from the shared secret, encrypt their identities, and exchange their encrypted identity information for authentication.

In contrast, aggressive mode only takes three steps to establish an IKE SA.

Step 1: The NBG420N sends its proposals to the remote IPSec router. It also starts the Diffie-Hellman key exchange and sends its (unencrypted) identity to the remote IPSec router for authentication.

Step 2: The remote IPSec router selects an acceptable proposal and sends it back to the NBG420N. It also finishes the Diffie-Hellman key exchange, authenticates the NBG420N, and sends its (unencrypted) identity to the NBG420N for authentication.

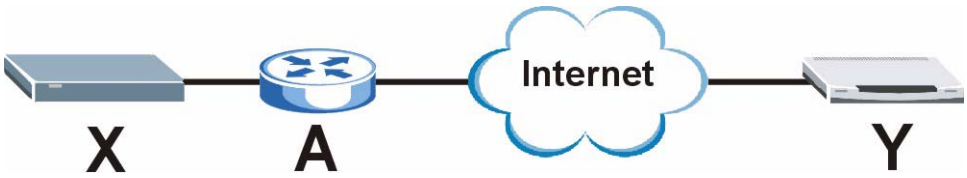
Step 3: The NBG420N authenticates the remote IPSec router and confirms that the IKE SA is established.

Aggressive mode does not provide as much security as main mode because the identity of the NBG420N and the identity of the remote IPSec router are not encrypted. It is usually used when the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication (for example, telecommuters).

VPN, NAT, and NAT Traversal

In the following example, there is another router (**A**) between router **X** and router **Y**.

Figure 114 VPN/NAT Example



If router **A** does NAT, it might change the IP addresses, port numbers, or both. If router **X** and router **Y** try to establish a VPN tunnel, the authentication fails because it depends on this information. The routers cannot establish a VPN tunnel.

Most routers like router **A** now have an IPSec pass-through feature. This feature helps router **A** recognize VPN packets and route them appropriately. If router **A** has this feature, router **X** and router **Y** can establish a VPN tunnel as long as the IPSec protocol is ESP. (See IPSec Protocol on page 188 for more information about active protocols.)

If router **A** does not have an IPSec pass-through or if the IPSec protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router **X** and router **Y** add an extra header to the IKE SA and IPSec SA packets. If you configure router **A** to forward these packets unchanged, router **X** and router **Y** can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the NBG420N and remote IPSec router.
- Configure the NAT router to forward packets with the extra header unchanged.

The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the NBG420N and remote IPSec router support.

IPSec Protocol

The IPSec protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPSec VPN includes two IPSec protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

Note: The NBG420N and remote IPSec router must use the same IPSec protocol.

Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

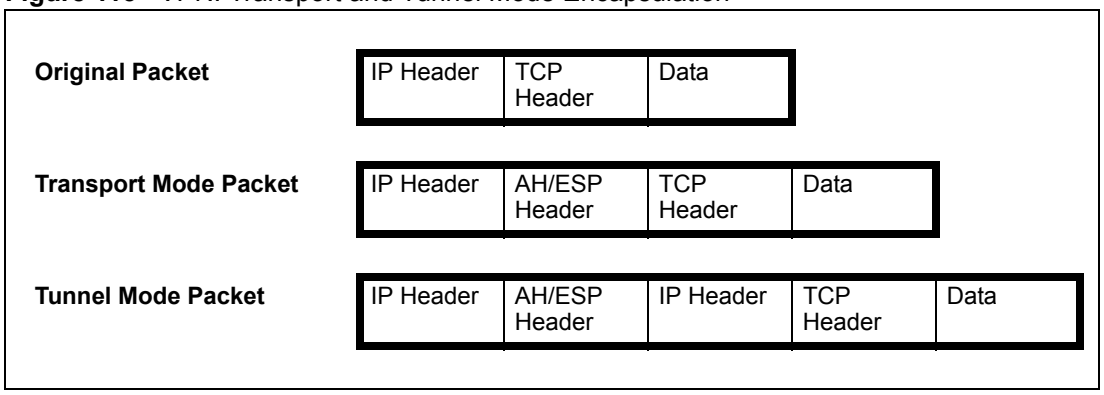
Encapsulation

There are two ways to encapsulate packets. Usually, you should use tunnel mode because it is more secure. Transport mode is only used when the IPSec SA is used for communication between the NBG420N and remote IPSec router (for example, for remote management), not between computers on the local and remote networks.

Note: The NBG420N and remote IPSec router must use the same encapsulation.

These modes are illustrated below.

Figure 115 VPN: Transport and Tunnel Mode Encapsulation



In tunnel mode, the NBG420N uses the IPSec protocol to encapsulate the entire IP packet. As a result, there are two IP headers:

- Outside header: The outside IP header contains the IP address of the NBG420N or remote IPSec router, whichever is the destination.
- Inside header: The inside IP header contains the IP address of the computer behind the NBG420N or remote IPSec router. The header for the IPSec protocol (AH or ESP) appears between the IP headers.

In transport mode, the encapsulation depends on the IPSec protocol. With AH, the NBG420N includes part of the original IP header when it encapsulates the packet. With ESP, however, the NBG420N does not include the IP header when it encapsulates the packet, so it is not possible to verify the integrity of the source IP address.

IPSec SA Proposal and Perfect Forward Secrecy

An IPSec SA proposal is similar to an IKE SA proposal (see IKE SA Proposal on page 185), except that you also have the choice whether or not the NBG420N and remote IPSec router perform a new DH key exchange every time an IPSec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the NBG420N and remote IPSec router perform a DH key exchange every time an IPSec SA is established, changing the root key from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys remain secure.

If you do not enable PFS, the NBG420N and remote IPSec router use the same root key that was generated when the IKE SA was established to generate encryption keys.

The DH key exchange is time-consuming and may be unnecessary for data that does not require such security.

Additional IPSec VPN Topics

This section discusses other IPSec VPN topics that apply to either IKE SAs or IPSec SAs or both. Relationships between the topics are also highlighted.

SA Life Time

SAs have a lifetime that specifies how long the SA lasts until it times out. When an SA times out, the NBG420N automatically renegotiates the SA in the following situations:

- There is traffic when the SA life time expires
- The IPSec SA is configured on the NBG420N as nailed up (see below)

Otherwise, the NBG420N must re-negotiate the SA the next time someone wants to send traffic.

Note: If the IKE SA times out while an IPSec SA is connected, the IPSec SA stays connected.

An IPSec SA can be set to **keep alive** Normally, the NBG420N drops the IPSec SA when the life time expires or after two minutes of outbound traffic with no inbound traffic. If you set the IPSec SA to keep alive , the NBG420N automatically renegotiates the IPSec SA when the SA life time expires, and it does not drop the IPSec SA if there is no inbound traffic.

Note: The SA life time and keep alive settings only apply if the rule identifies the remote IPSec router by a static IP address or a domain name. If the **Secure Gateway Address** field is set to **0.0.0.0**, the NBG420N cannot initiate the tunnel (and cannot renegotiate the SA).

Encryption and Authentication Algorithms

In most NBG420Ns, you can select one of the following encryption algorithms for each proposal. The encryption algorithms are listed here in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data.
- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.

You can select one of the following authentication algorithms for each proposal. The algorithms are listed here in order from weakest to strongest.

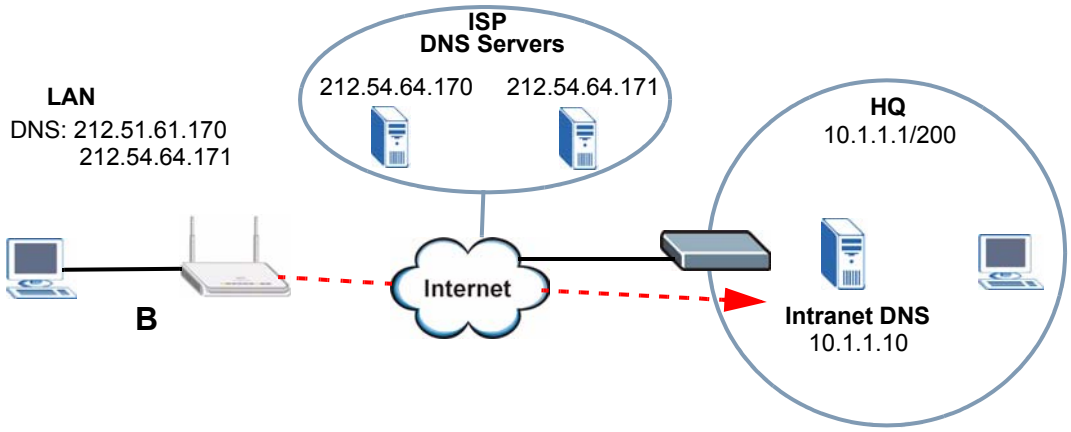
- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

Private DNS Server

In cases where you want to use domain names to access Intranet servers on a remote private network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote private network.

The following figure depicts an example where one VPN tunnel is created from an NBG420N at branch office (**B**) to headquarters (**HQ**). In order to access computers that use private domain names on the **HQ** network, the NBG420N at **B** uses the Intranet DNS server in headquarters.

Figure 116 Private DNS Server Example



If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote private network.

PART IV
Management

Static Route Screens (195)
Bandwidth Management (199)
Remote Management (209)
Universal Plug-and-Play (UPnP) (215)

16

Static Route Screens

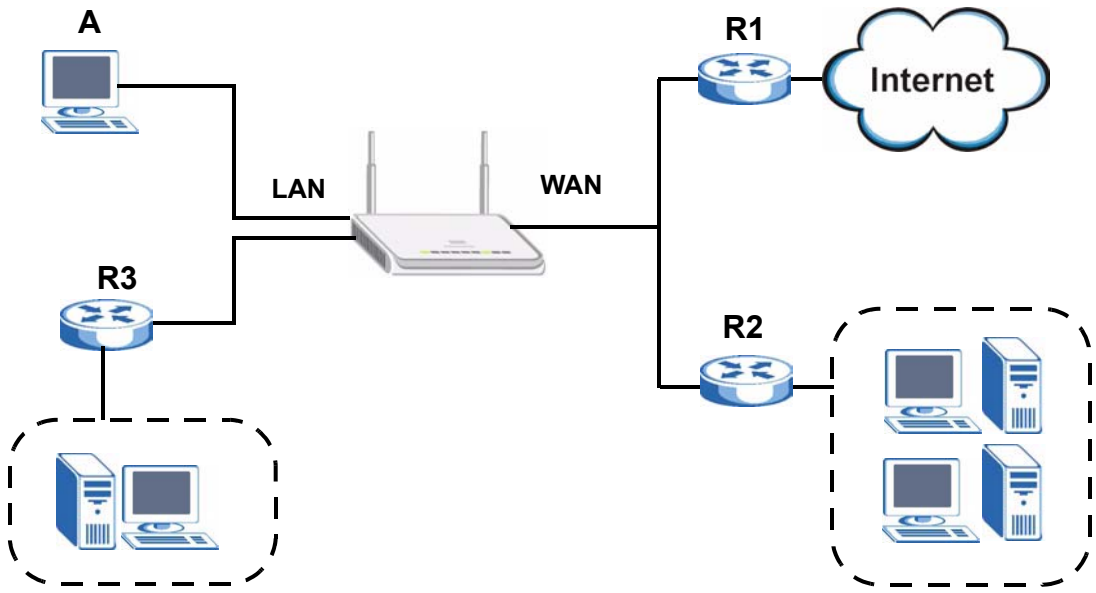
This chapter shows you how to configure static routes for your NBG420N.

16.1 Static Route Overview

The NBG420N usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the NBG420N send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the NBG420N's LAN interface. The NBG420N routes most traffic from **A** to the Internet through the NBG420N's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

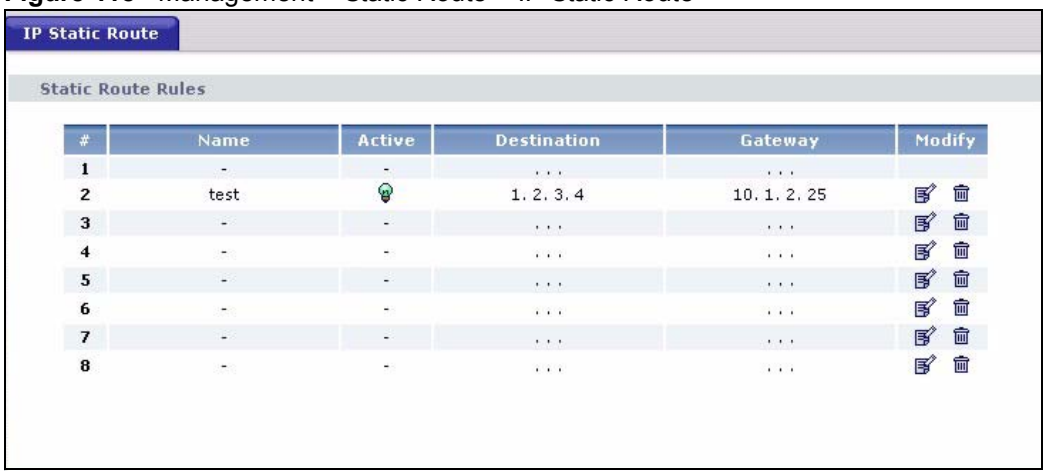
Figure 117 Example of Static Routing Topology



16.2 IP Static Route Screen

Click **Management** > **Static Route** to open the **IP Static Route** screen. The following screen displays.

Figure 118 Management > Static Route > IP Static Route



The following table describes the labels in this screen.

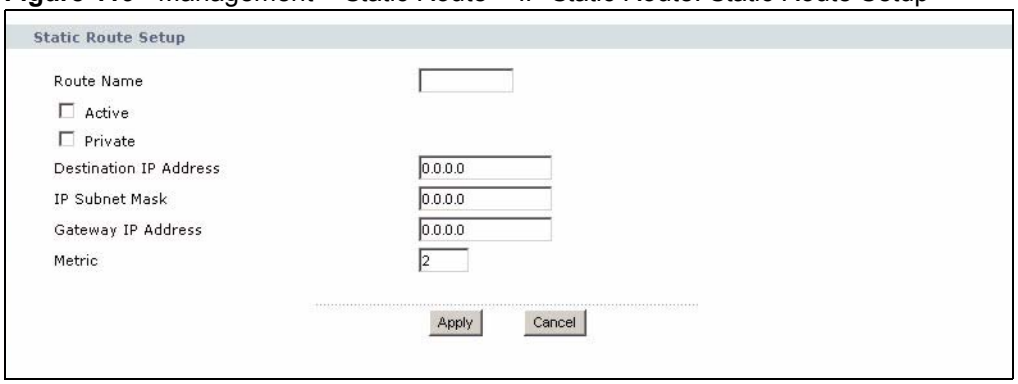
Table 69 Management > Static Route > IP Static Route

LABEL	DESCRIPTION
#	This is the index number of an individual static route. The first entry is for the default route and not editable.
Name	This is the name that describes or identifies this route.
Active	This icon is turned on when this static route is active. Click the **Edit** icon under **Modify** and select the **Active** checkbox in the **Static Route Setup** screen to enable the static route. Clear the checkbox to disable this static route without having to delete the entry.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is an immediate neighbor of your NBG420N that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your NBG420N; over the WAN, the gateway must be the IP address of one of the remote nodes.
Modify	Click the **Edit** icon to open the static route setup screen. Modify a static route or create a new static route in the **Static Route Setup** screen. Click the **Remove** icon to delete a static route.

16.2.1 Static Route Setup Screen

To edit a static route, click the edit icon under **Modify**. The following screen displays. Fill in the required information for each static route.

Figure 119 Management > Static Route > IP Static Route: Static Route Setup



The following table describes the labels in this screen.

Table 70 Management > Static Route > IP Static Route: Static Route Setup

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Private	This parameter determines if the NBG420N will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this checkbox to propagate this route to other hosts through RIP broadcasts.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your NBG420N that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your NBG420N; over the WAN, the gateway must be the IP address of one of the Remote Nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Apply	Click **Apply** to save your changes back to the NBG420N.
Cancel	Click **Cancel** to return to the previous screen and not save your changes.

17

Bandwidth Management

This chapter contains information about configuring bandwidth management, editing rules and viewing the NBG420N's bandwidth management logs.

17.1 Bandwidth Management Overview

ZyXEL's Bandwidth Management allows you to specify bandwidth management rules based on an application and/or subnet. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth rules.

The NBG420N applies bandwidth management to traffic that it forwards out through an interface. The NBG420N does not control the bandwidth of traffic that comes into an interface.

Bandwidth management applies to all traffic flowing out of the router, regardless of the traffic's source.

Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the NBG420N and be managed by bandwidth management.

- The sum of the bandwidth allotments that apply to the WAN interface (LAN to WAN, WLAN to WAN, WAN to WAN / NBG420N) must be less than or equal to the **Upstream Bandwidth** that you configure in the **Bandwidth Management Advanced** screen.
- The sum of the bandwidth allotments that apply to the LAN port (WAN to LAN, WLAN to LAN, LAN to LAN / NBG420N) must be less than or equal to 100,000 kbps (you cannot configure the bandwidth budget for the LAN port).
- The sum of the bandwidth allotments that apply to the WLAN port (LAN to WLAN, WAN to WLAN, WLAN to WLAN / NBG420N) must be less than or equal to 54,000 kbps (you cannot configure the bandwidth budget for the WLAN port).

17.2 Application-based Bandwidth Management

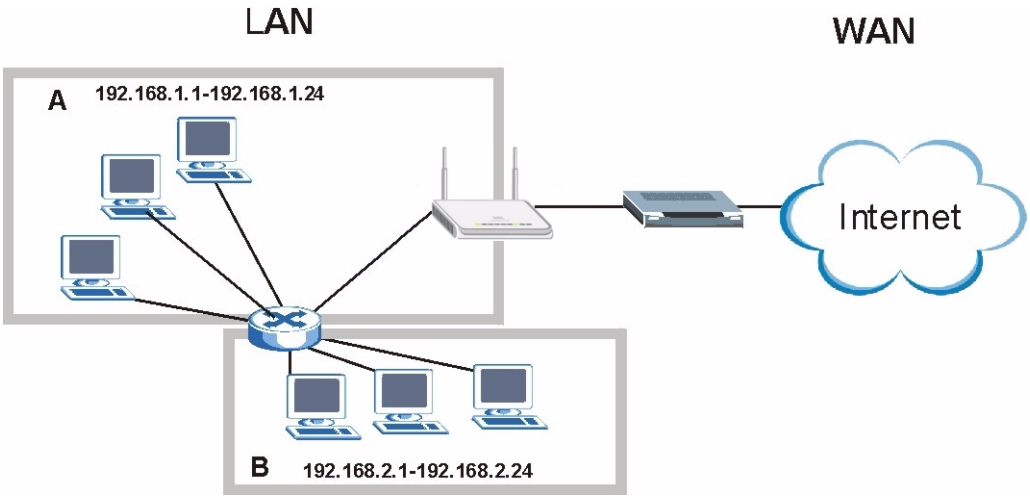
You can create bandwidth classes based on individual applications (like VoIP, Web, FTP, E-mail and Video for example).

17.3 Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets.

The following figure shows LAN subnets. You could configure one bandwidth class for subnet **A** and another for subnet **B**.

Figure 120 Subnet-based Bandwidth Management Example



17.4 Application and Subnet-based Bandwidth Management

You could also create bandwidth classes based on a combination of a subnet and an application. The following example table shows bandwidth allocations for application specific traffic from separate LAN subnets.

Table 71 Application and Subnet-based Bandwidth Management Example

TRAFFIC TYPE	FROM SUBNET A	FROM SUBNET B
VoIP	64 Kbps	64 Kbps
Web	64 Kbps	64 Kbps
FTP	64 Kbps	64 Kbps
E-mail	64 Kbps	64 Kbps
Video	64 Kbps	64 Kbps

17.5 Bandwidth Management Priorities

The following table describes the priorities that you can apply to traffic that the NBG420N forwards out through an interface.

Table 72 Bandwidth Management Priorities

PRIORITY LEVELS: TRAFFIC WITH A HIGHER PRIORITY GETS THROUGH FASTER WHILE TRAFFIC WITH A LOWER PRIORITY IS DROPPED IF THE NETWORK IS CONGESTED.	
High	Typically used for voice traffic or video that is especially sensitive to jitter (jitter is the variations in delay).

Table 72 Bandwidth Management Priorities

PRIORITY LEVELS: TRAFFIC WITH A HIGHER PRIORITY GETS THROUGH FASTER WHILE TRAFFIC WITH A LOWER PRIORITY IS DROPPED IF THE NETWORK IS CONGESTED.	
Mid	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Low	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.

17.6 Predefined Bandwidth Management Services

The following is a description of the services that you can select and to which you can apply media bandwidth management using the wizard screens.

Table 73 Media Bandwidth Management Setup: Services

SERVICE	DESCRIPTION
Xbox Live	This is Microsoft’s online gaming service that lets you play multiplayer Xbox games on the Internet via broadband technology. Xbox Live uses port 3074.
VoIP (SIP)	Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is transported primarily over UDP but can also be transported over TCP, using the default port number 5060.
FTP	File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail. FTP uses port number 21.
E-Mail	Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80
BitTorrent	BitTorrent is a free P2P (peer-to-peer) sharing tool allowing you to distribute large software and media files using ports 6881 to 6889. BitTorrent requires you to search for a file with a searching engine yourself. It distributes files by corporation and trading, that is, the client downloads the file in small pieces and share the pieces with other peers to get other half of the file.
MSN Webcam	MSN messenger allows you to chat online and send instant messages. If you use MSN messenger and also have a webcam, you can send your image/photo in real-time along with messages
WWW	The World Wide Web (WWW) is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser.

17.6.1 Services and Port Numbers

See Appendix F on page 321 for commonly used services and port numbers.

17.7 Default Bandwidth Management Classes and Priorities

If you enable bandwidth management but do not configure a rule for critical traffic like VoIP, the voice traffic may then get delayed due to insufficient bandwidth. With the automatic traffic classifier feature activated, the NBG420N automatically assigns a default bandwidth management class and priority to traffic that does not match any of the user-defined rules. The traffic is classified based on the traffic type. Real-time traffic always gets higher priority over other traffic.

The following table shows you the priorities between the three default classes (**AutoClass_H**, **AutoClass_M** and **Default Class**) and user-defined rules. 6 is the highest priority.

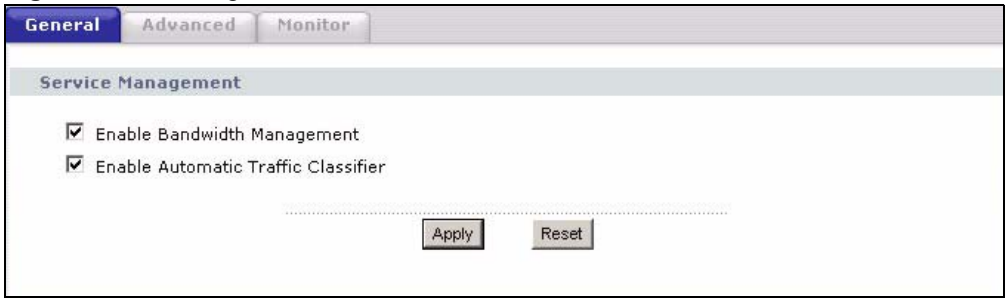
Table 74 Bandwidth Management Priority with Default Classes

CLASS TYPE	PRIORITY
User-defined with high priority	6
AutoClass_H	5
User-defined with medium priority	4
AutoClass_M	3
User-defined with low priority	2
Default Class	1

17.8 Bandwidth Management General Configuration

Click **Management > Bandwidth MGMT** to open the bandwidth management **General** screen.

Figure 121 Management > Bandwidth MGMT > General



The following table describes the labels in this screen.

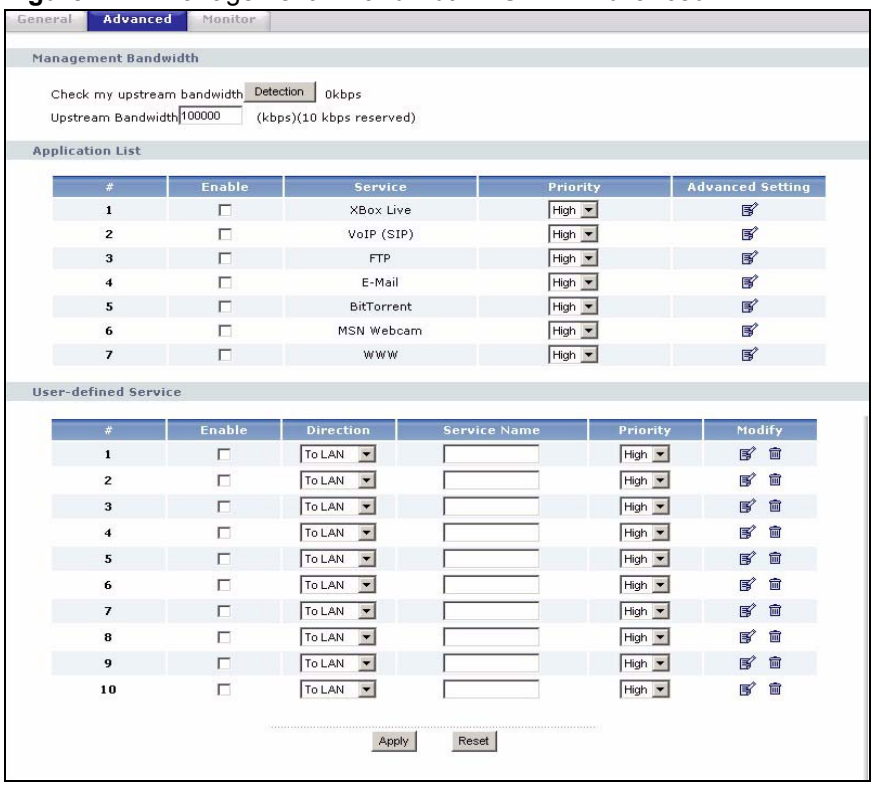
Table 75 Management > Bandwidth MGMT > General

LABEL	DESCRIPTION
Enable Bandwidth Management	Select this check box to have the NBG420N apply bandwidth management. Enable bandwidth management to give traffic that matches a bandwidth rule priority over traffic that does not match a bandwidth rule. Enabling bandwidth management also allows you to control the maximum or minimum amounts of bandwidth that can be used by traffic that matches a bandwidth rule.
Enable Automatic Traffic Classifier	This field is only applicable when you select the **Enable Bandwidth Management** check box. Select this check box to have the NBG420N base on the default bandwidth classes to apply bandwidth management. Real-time packets, such as VoIP traffic always get higher priority.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

17.9 Bandwidth Management Advanced Configuration

Click **Management** > **Bandwidth MGMT** > **Advanced** to open the bandwidth management **Advanced** screen.

Figure 122 Management > Bandwidth MGMT > Advanced



The following table describes the labels in this screen.

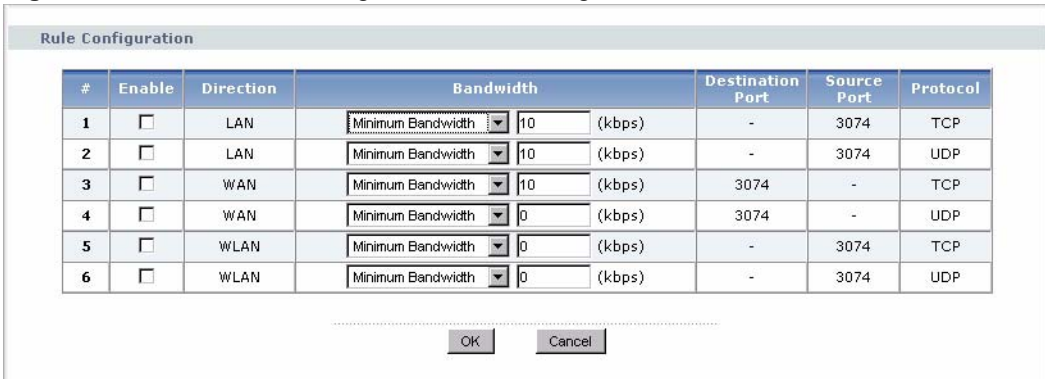
Table 76 Management > Bandwidth MGMT > Advanced

LABEL	DESCRIPTION
Check my upstream bandwidth	Click the **Detection** button to check the size of your upstream bandwidth.
Upstream Bandwidth (kbps)	Enter the amount of bandwidth in kbps (2 to 100,000) that you want to allocate for traffic. 20 kbps to 20,000 kbps is recommended. The recommendation is to set this speed to be equal to or less than the speed of the broadband device connected to the WAN port. For example, set the speed to 1000 Kbps (or less) if the broadband device connected to the WAN port has an upstream speed of 1000 Kbps.
Application List	Use this table to allocate specific amounts of bandwidth based on the pre-defined service.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the NBG420N apply this bandwidth management rule.
Service	This is the name of the service.
Priority	Select a priority from the drop down list box. Choose **High**, **Mid** or **Low**.
Advanced Setting	Click the **Edit** icon to open the **Rule Configuration** screen where you can modify the rule.
User-defined Service	Use this table to allocate specific amounts of bandwidth to specific applications and/or subnets.
#	This is the number of an individual bandwidth management rule.
Enable	Select this check box to have the NBG420N apply this bandwidth management rule.
Direction	Select **To LAN** to apply bandwidth management to traffic that the NBG420N forwards to the LAN. Select **To WAN** to apply bandwidth management to traffic that the NBG420N forwards to the WAN. Select **To WLAN** to apply bandwidth management to traffic that the NBG420N forwards to the WLAN.
Service Name	Enter a descriptive name of up to 19 alphanumeric characters, including spaces.
Priority	Select a priority from the drop down list box. Choose **High**, **Mid** or **Low**.
Modify	Click the **Edit** icon to open the **Rule Configuration** screen. Modify an existing rule or create a new rule in the **Rule Configuration** screen. See Section 17.9.2 on page 205 for more information. Click the **Remove** icon to delete a rule.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

17.9.1 Rule Configuration with the Pre-defined Service

To edit a bandwidth management rule for the pre-defined service in the NBG420N, click the **Edit** icon in the **Application List** table of the **Advanced** screen. The following screen displays.

Figure 123 Bandwidth Management Rule Configuration: Pre-defined Service


Rule Configuration
Enable Direction Bandwidth Destination Port Source Port Protocol
1 LAN Minimum Bandwidth 10 (kbps) - 3074 TCP
2 LAN Minimum Bandwidth 10 (kbps) - 3074 UDP
3 WAN Minimum Bandwidth 10 (kbps) 3074 - TCP
4 WAN Minimum Bandwidth 0 (kbps) 3074 - UDP
5 WLAN Minimum Bandwidth 0 (kbps) - 3074 TCP
6 WLAN Minimum Bandwidth 0 (kbps) - 3074 UDP
OK
Cancel

The following table describes the labels in this screen.

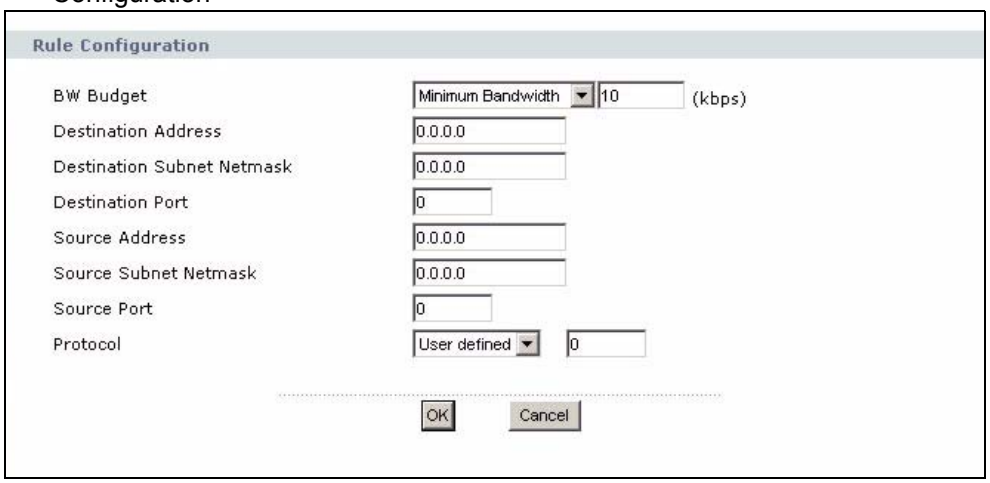
Table 77 Bandwidth Management Rule Configuration: Pre-defined Service

LABEL	DESCRIPTION
#	This is the number of an individual bandwidth management rule.
Enable	Select an interface's check box to enable bandwidth management on that interface.
Direction	These read-only labels represent the physical interfaces. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the NBG420N and be managed by bandwidth management.
Bandwidth	Select **Maximum Bandwidth** or **Minimum Bandwidth** and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second.
Destination Port	This is the port number of the destination. See Appendix F on page 321 for some common services and port numbers.
Source Port	This is the port number of the source. See Appendix F on page 321 for some common services and port numbers.
Protocol	This is the protocol (**TCP** or **UDP**) used for the service.
OK	Click **OK** to save your customized settings.
Cancel	Click **Cancel** to exit this screen without saving.

17.9.2 Rule Configuration: User Defined Service Rule Configuration

If you want to edit a bandwidth management rule for other applications and/or subnets, click the **Edit** icon in the **User-defined Service** table of the **Advanced** screen. The following screen displays.

Figure 124 Management > Bandwidth MGMT > Advanced: User-defined Service Rule Configuration



The following table describes the labels in this screen

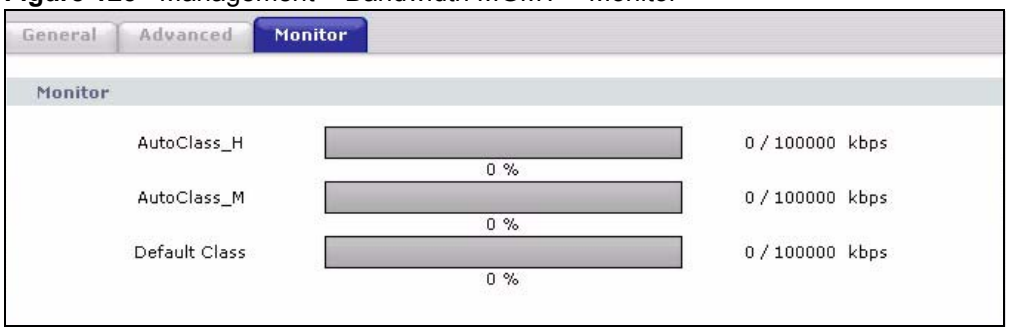
Table 78 Management > Bandwidth MGMT > Advanced: User-defined Service Rule Configuration

LABEL	DESCRIPTION
BW Budget	Select **Maximum Bandwidth** or **Minimum Bandwidth** and specify the maximum or minimum bandwidth allowed for the rule in kilobits per second.
Destination Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a **Destination Address**. Refer to the appendices for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See *Appendix F on page 321* for some common services and port numbers.
Source Address	Enter the source IP address in dotted decimal notation.
Source Subnet Netmask	Enter the destination subnet mask. This field is N/A if you do not specify a **Source Address**. Refer to the appendices for more information on IP subnetting.
Source Port	Enter the port number of the source. See Appendix F on page 321 for some common services and port numbers.
Protocol	Select the protocol (**TCP** or **UDP**) or select **User defined** and enter the protocol (service type) number.
OK	Click **OK** to save your customized settings.
Cancel	Click **Cancel** to exit this screen without saving.

17.10 Bandwidth Management Monitor

Click **Management > Bandwidth MGMT** > **Monitor** to open the bandwidth management **Monitor** screen. View the bandwidth usage of the WAN configured bandwidth rules. This is also shown as bandwidth usage over the bandwidth budget for each rule. The gray section of the bar represents the percentage of unused bandwidth and the blue color represents the percentage of bandwidth in use.

Figure 125 Management > Bandwidth MGMT > Monitor



18

Remote Management

This chapter provides information on the Remote Management screens.

18.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which NBG420N interface (if any) from which computers.

When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.

You may manage your NBG420N from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN and WAN)
- Neither (Disable).

When you choose **WAN** or **LAN & WAN**, you still need to configure a firewall rule to allow access.

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

You may only have one remote management session running at a time. The NBG420N automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. Telnet
2. HTTP

18.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. You have disabled that service in one of the remote management screens.
2. The IP address in the **Secured Client IP Address** field does not match the client IP address. If it does not match, the NBG420N will disconnect the session immediately.
3. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
4. There is a firewall rule that blocks it.

18.1.2 Remote Management and NAT

When NAT is enabled:

- Use the NBG420N's WAN IP address when configuring from the WAN.
- Use the NBG420N's LAN IP address when configuring from the LAN.

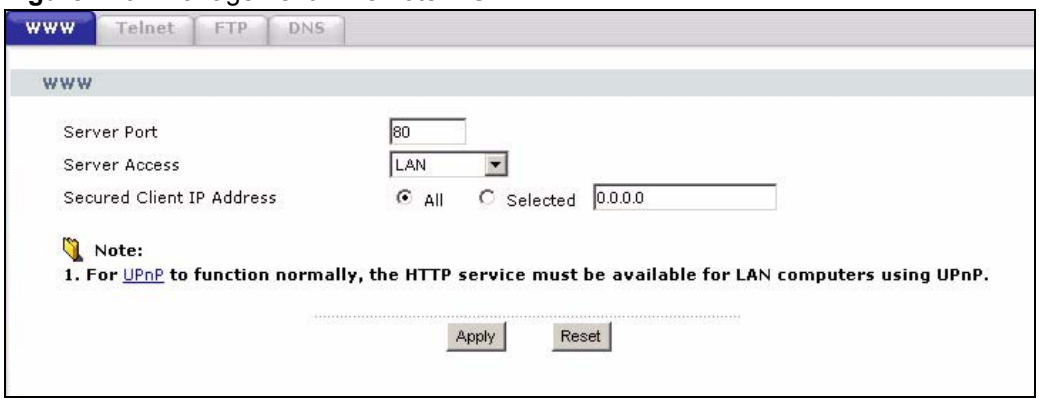
18.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The NBG420N automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen

18.2 WWW Screen

To change your NBG420N's World Wide Web settings, click **Management** > **Remote MGMT** to display the **WWW** screen.

Figure 126 Management > Remote MGMT > WWW



The following table describes the labels in this screen

Table 79 Management > Remote MGMT > WWW

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NBG420N using this service.

LABEL	DESCRIPTION
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the NBG420N using this service. Select **All** to allow any computer to access the NBG420N using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the NBG420N using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

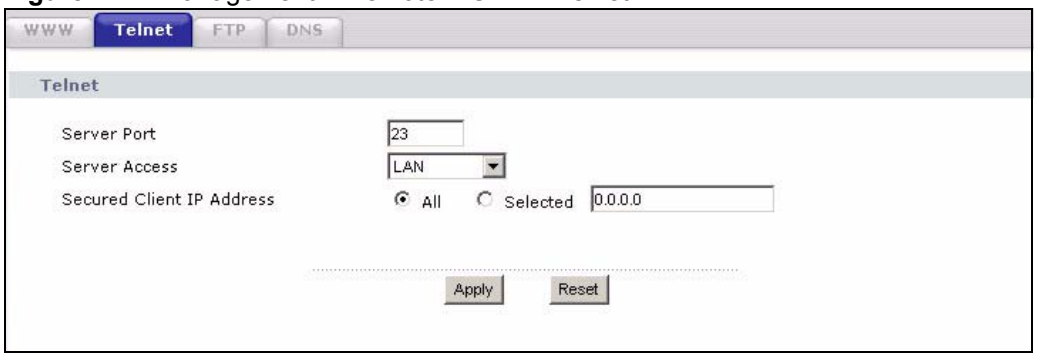
18.3 Telnet

You can use Telnet to access the NBG420N’s command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

18.4 Telnet Screen

To change your NBG420N’s Telnet settings, click **Management** > **Remote MGMT** > **Telnet**. The following screen displays.

Figure 127 Management > Remote MGMT > Telnet



The following table describes the labels in this screen.

Table 80 Management > Remote MGMT > Telnet

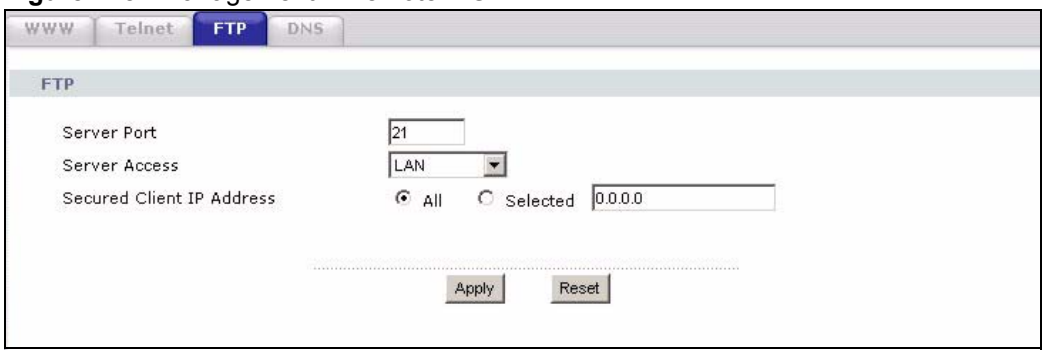
LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NBG420N using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the NBG420N using this service. Select **All** to allow any computer to access the NBG420N using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the NBG420N using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

18.5 FTP Screen

You can use FTP (File Transfer Protocol) to upload and download the NBG420N's firmware and configuration files. To use this feature, your computer must have an FTP client.

To change your NBG420N's FTP settings, click **Management** > **Remote MGMT** > **FTP**. The screen appears as shown. Use this screen to specify which interfaces allow FTP access and from which IP address the access can come.

Figure 128 Management > Remote MGMT > FTP



The following table describes the labels in this screen.

Table 81 Management > Remote MGMT > FTP

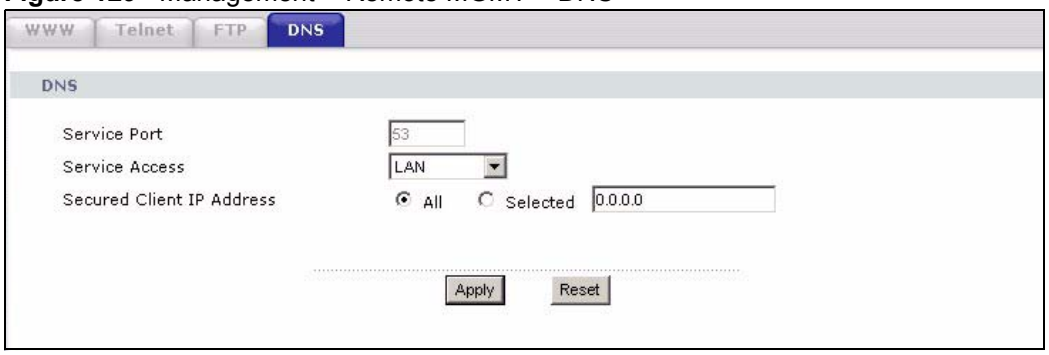
LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the NBG420N using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the NBG420N using this service. Select **All** to allow any computer to access the NBG420N using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the NBG420N using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

18.6 DNS Screen

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to the chapter on Wizard Setup for background information.

To change your NBG420N's DNS settings, click **Management** > **Remote MGMT** > **DNS**. The screen appears as shown.

Figure 129 Management > Remote MGMT > DNS



The following table describes the labels in this screen.

Table 82 Management > Remote MGMT > DNS

LABEL	DESCRIPTION
Server Port	The DNS service port number is 53 and cannot be changed here.
Server Access	Select the interface(s) through which a computer may send DNS queries to the NBG420N.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to send DNS queries to the NBG420N. Select **All** to allow any computer to send DNS queries to the NBG420N. Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the NBG420N.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

19

Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

19.1 Introducing Universal Plug and Play

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

See Section 19.3 on page 216 for configuration instructions.

19.1.1 How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

19.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

19.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the NBG420N allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

19.2 UPnP and ZyXEL

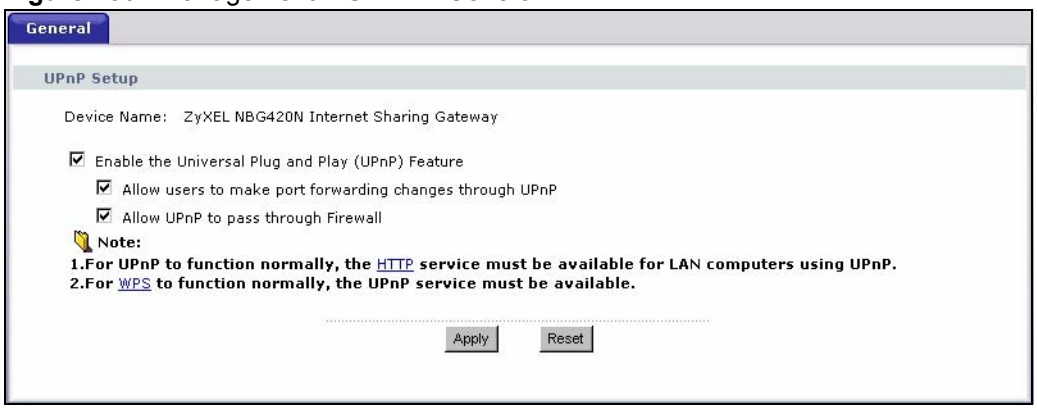
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See the following sections for examples of installing and using UPnP.

19.3 UPnP Screen

Click the **Management > UPnP** to display the UPnP screen.

Figure 130 Management > UPnP > General


General
UPnP Setup
Device Name: ZyXEL NBG420N Internet Sharing Gateway
Enable the Universal Plug and Play (UPnP) Feature
Allow users to make port forwarding changes through UPnP
Allow UPnP to pass through Firewall
Note:
1.For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.
2.For WPS to function normally, the UPnP service must be available.
Apply
Reset

The following table describes the labels in this screen.

Table 83 Management > UPnP > General

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Feature	Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the NBG420N's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the NBG420N so that they can communicate through the NBG420N, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through Firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).

Table 83 Management > UPnP > General

LABEL	DESCRIPTION
Apply	Click **Apply** to save the setting to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

19.4 Installing UPnP in Windows Example

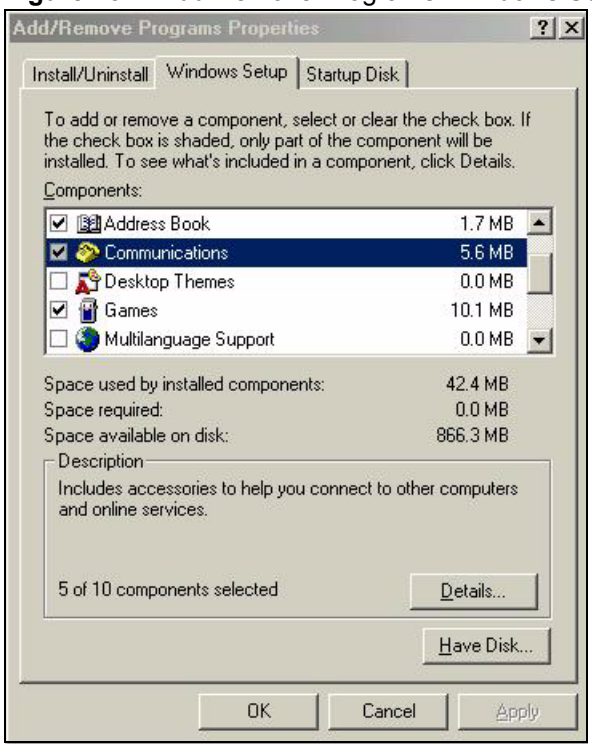
This section shows how to install UPnP in Windows Me and Windows XP.

19.4.0.1 Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

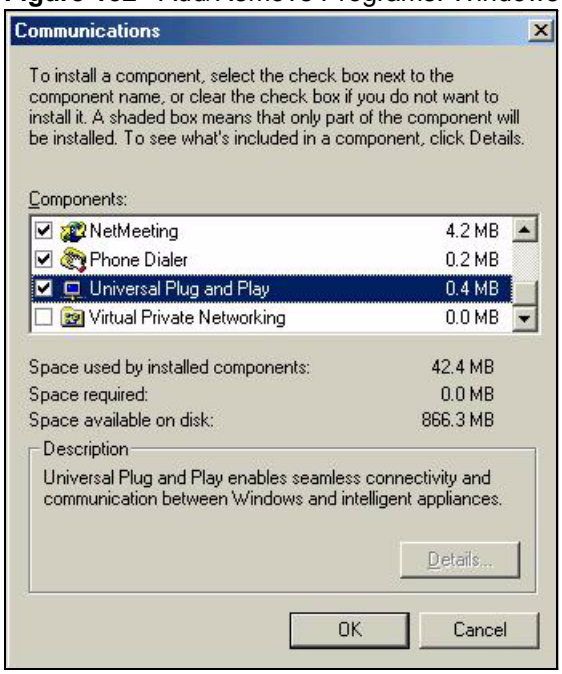
1. Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
2. Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 131 Add/Remove Programs: Windows Setup: Communication


Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.
Components:
Address Book 1.7 MB
Communications 5.6 MB
Desktop Themes 0.0 MB
Games 10.1 MB
Multilanguage Support 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Includes accessories to help you connect to other computers and online services.
5 of 10 components selected
Details...
Have Disk...
OK
Cancel
Apply

3. In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 132 Add/Remove Programs: Windows Setup: Communication: Components


Communications
To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
NetMeeting 4.2 MB
Phone Dialer 0.2 MB
Universal Plug and Play 0.4 MB
Virtual Private Networking 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

1 Click **Start** and **Control Panel**.

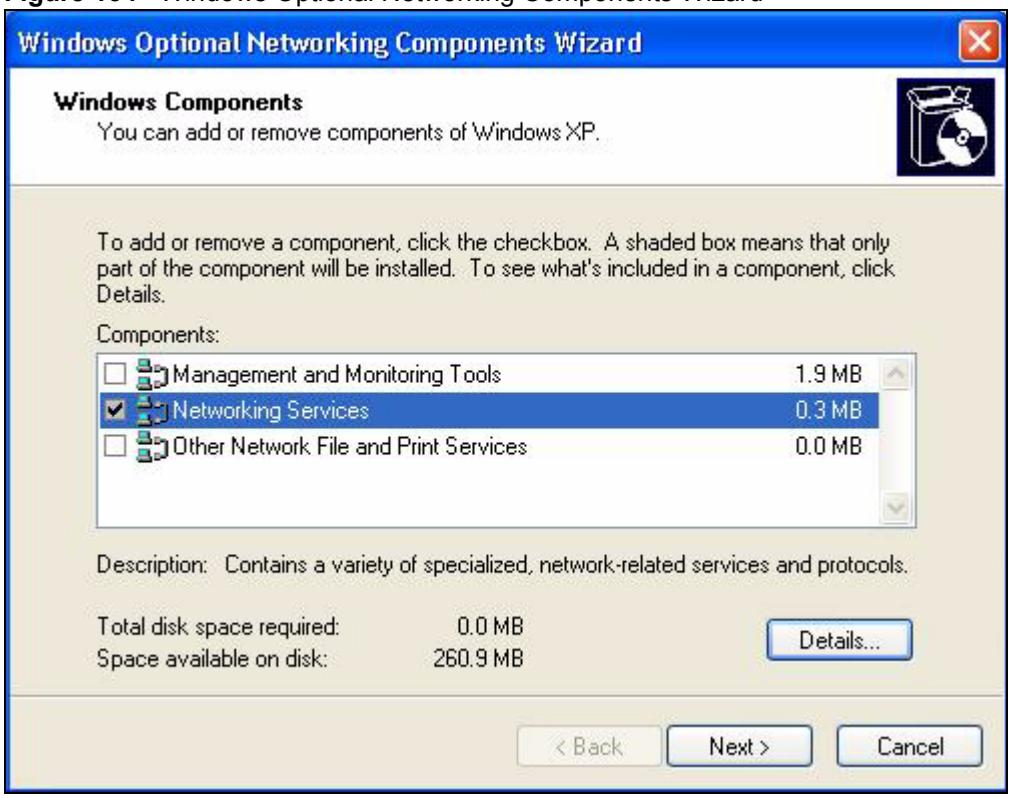
2 Double-click **Network Connections**.

3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.

Figure 133 Network Connections

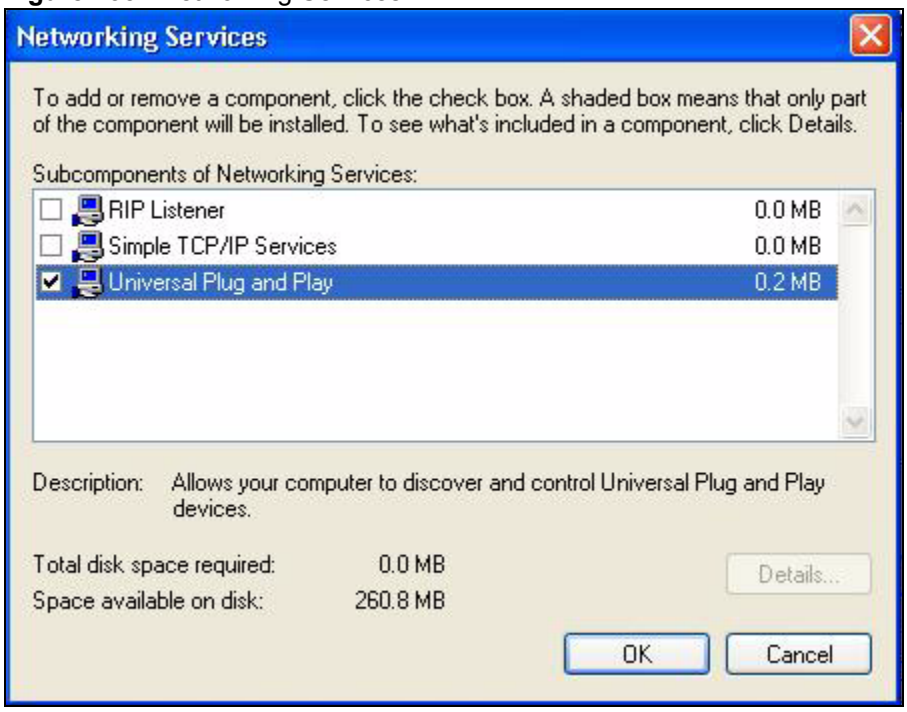
4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 134 Windows Optional Networking Components Wizard


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 1.9 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 260.9 MB
Details...
< Back
Next >
Cancel

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 135 Networking Services


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Allows your computer to discover and control Universal Plug and Play devices.
Total disk space required: 0.0 MB
Space available on disk: 260.8 MB
Details...
OK
Cancel

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

19.4.0.2 Using UPnP in Windows XP Example

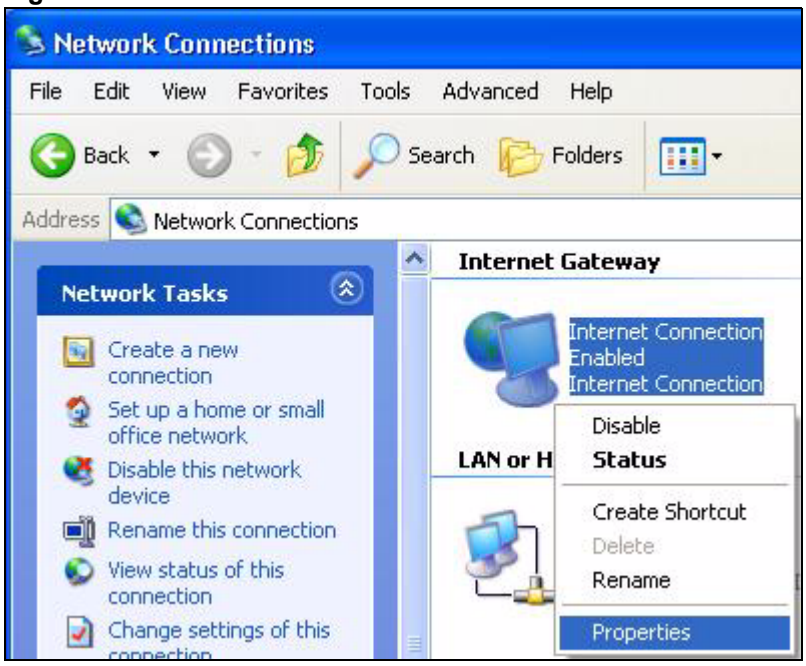
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the NBG420N.

Make sure the computer is connected to a LAN port of the NBG420N. Turn on your computer and the NBG420N.

Auto-discover Your UPnP-enabled Network Device

1. Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
2. Right-click the icon and select **Properties**.

Figure 136 Network Connections



3. In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 137 Internet Connection Properties

Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 138 Internet Connection Properties: Advanced Settings

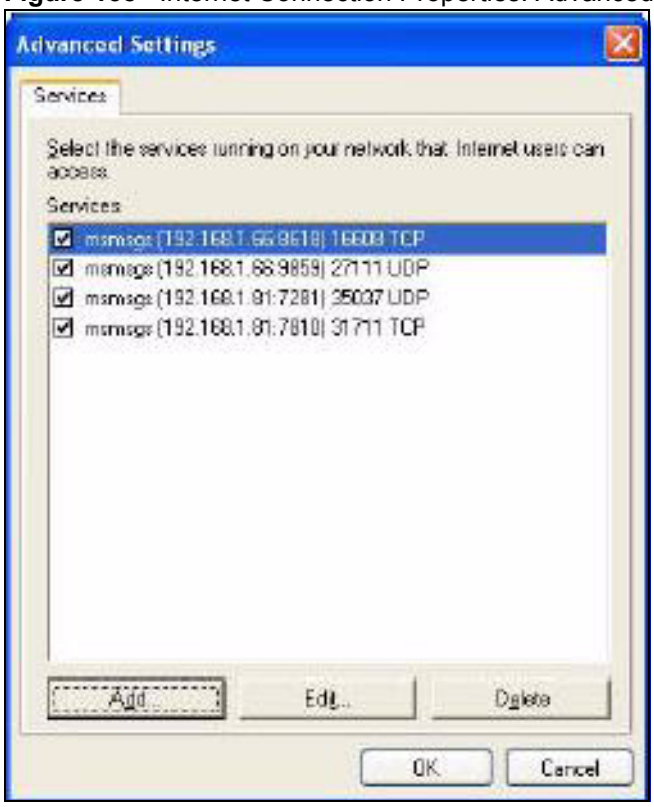
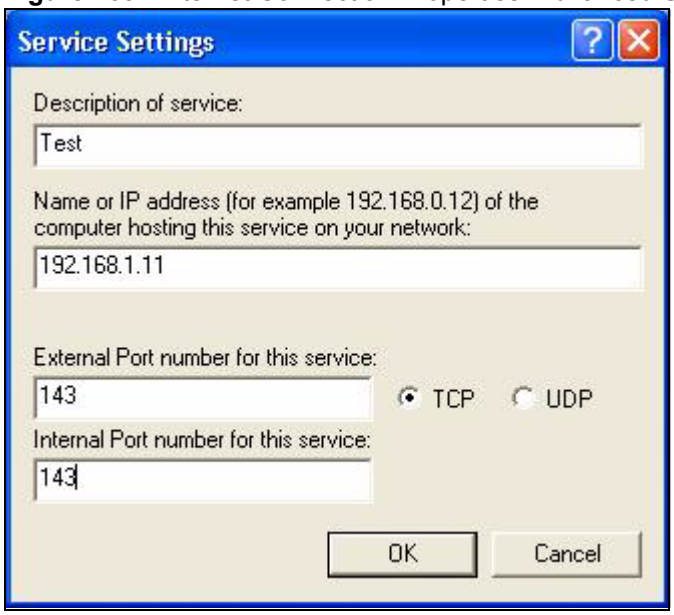


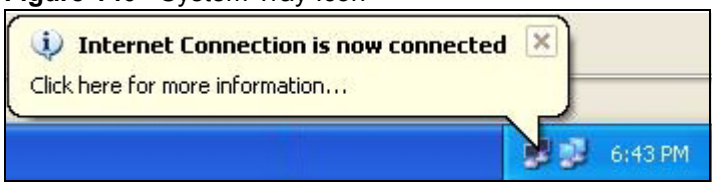
Figure 139 Internet Connection Properties: Advanced Settings: Add



5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 140 System Tray Icon



7 Double-click on the icon to display your current Internet connection status.

Figure 141 Internet Connection Status

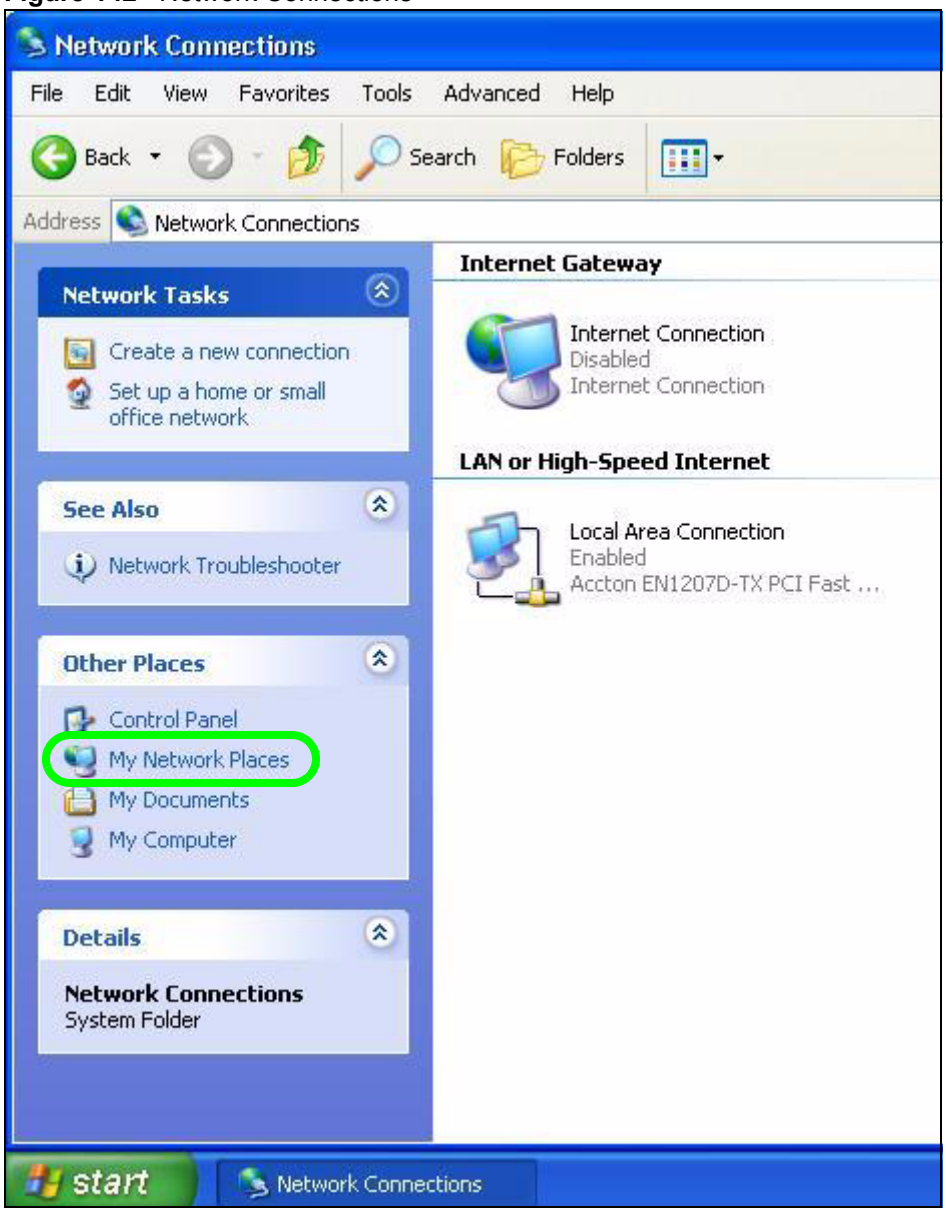
Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the NBG420N without finding out the IP address of the NBG420N first. This comes helpful if you do not know the IP address of the NBG420N.

Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.
2 Double-click **Network Connections**.
3 Select **My Network Places** under **Other Places**.

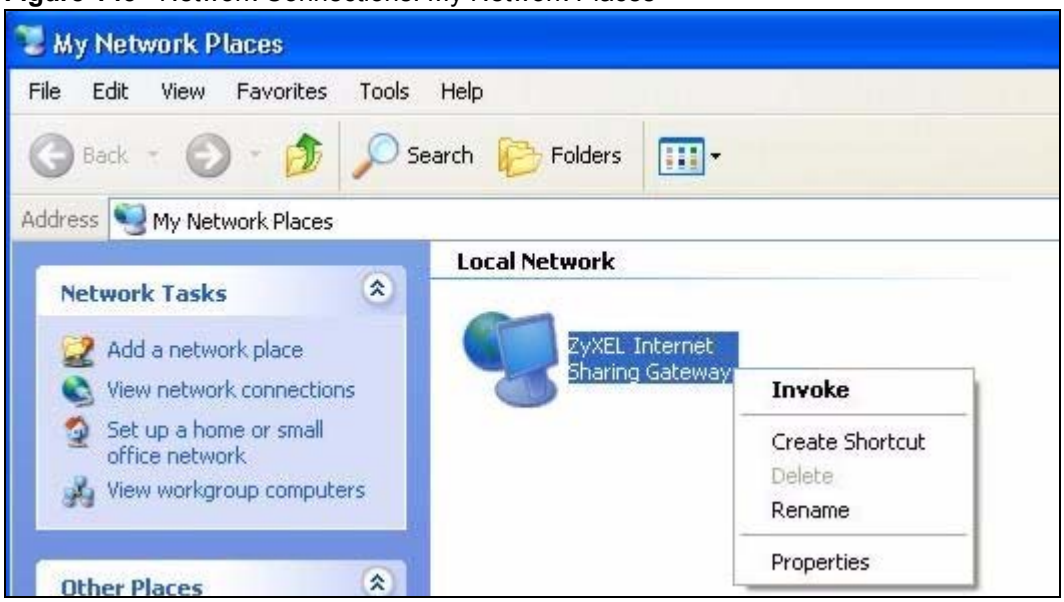
Figure 142 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your NBG420N and select **Invoke**. The web configurator login screen displays.

Figure 143 Network Connections: My Network Places



6 Right-click on the icon for your NBG420N and select **Properties**. A properties window displays with basic information about the NBG420N.

Figure 144 Network Connections: My Network Places: Properties: Example

PART V
Maintenance and Troubleshooting

System (229)
Logs (233)
Tools (251)
Configuration Mode (257)
Sys Op Mode (259)
Language (263)
Troubleshooting (265)

20 System

This chapter provides information on the **System** screens.

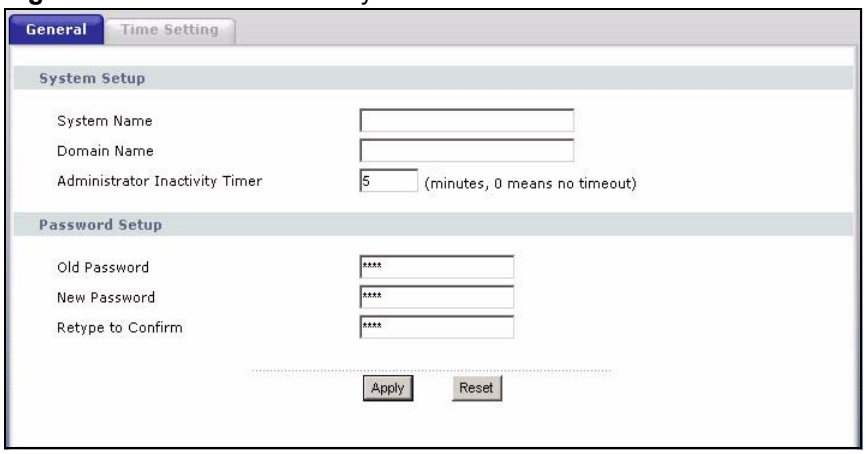
20.1 System Overview

See the chapter about wizard setup for more information on the next few screens.

20.2 System General Screen

Click **Maintenance** > **System**. The following screen displays.

Figure 145 Maintenance > System > General



The following table describes the labels in this screen.

Table 84 Maintenance > System > General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the NBG420N in an Ethernet network. It is recommended you enter your computer's "Computer name" in this field (see the chapter about wizard setup for how to find your computer's name). This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.

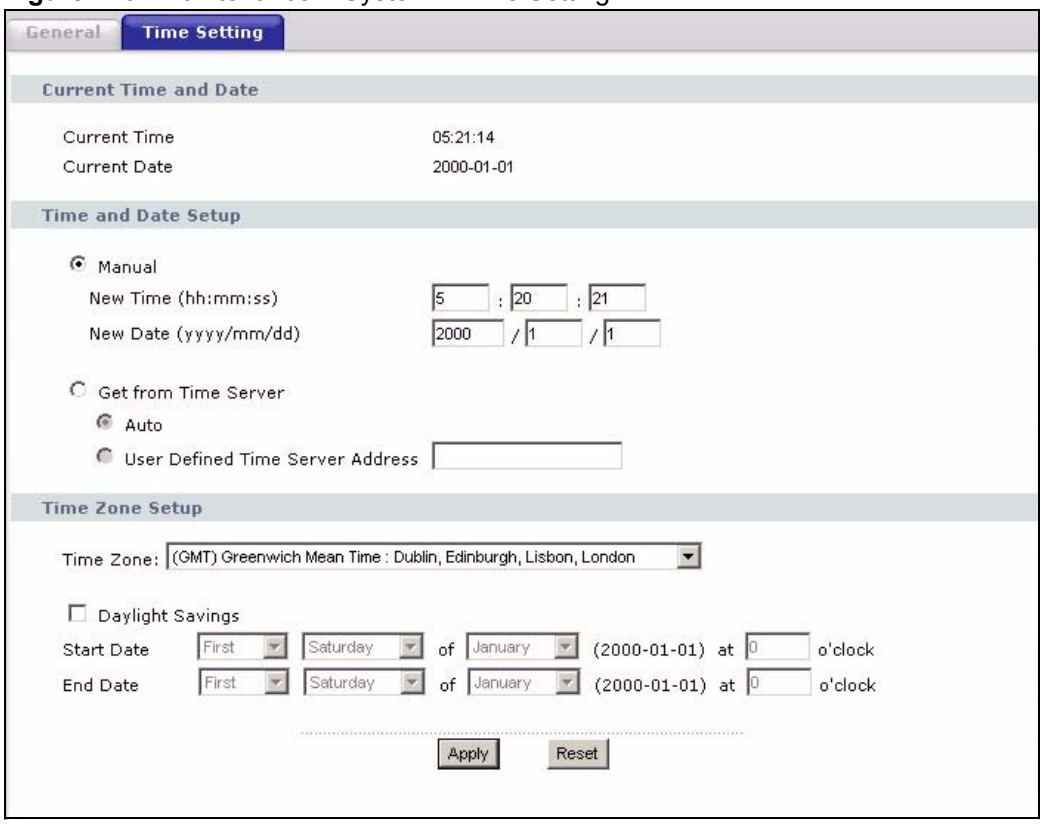
Table 84 Maintenance > System > General

LABEL	DESCRIPTION
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Password Setup	Change your NBG420N's password (recommended) using the fields as shown.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

20.3 Time Setting Screen

To change your NBG420N's time and date, click **Maintenance** > **System** > **Time Setting**. The screen appears as shown. Use this screen to configure the NBG420N's time based on your local time zone.

Figure 146 Maintenance > System > Time Setting



The following table describes the labels in this screen.

Table 85 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your NBG420N. Each time you reload this page, the NBG420N synchronizes the time with the time server.
Current Date	This field displays the date of your NBG420N. Each time you reload this page, the NBG420N synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**.
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the NBG420N get the time and date from the time server you specified below.
Auto	Select **Auto** to have the NBG420N automatically search for an available time server and synchronize the date and time with the time server after you click **Apply**.
User Defined Time Server Address	Select **User Defined Time Server Address** and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **April** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 85 Maintenance > System > Time Setting

LABEL	DESCRIPTION
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Last**, **Sunday**, **October** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes back to the NBG420N.
Reset	Click **Reset** to begin configuring this screen afresh.

21

Logs

This chapter contains information about configuring general log settings and viewing the NBG420N's logs. Refer to the appendices for example log message explanations.

21.1 View Log

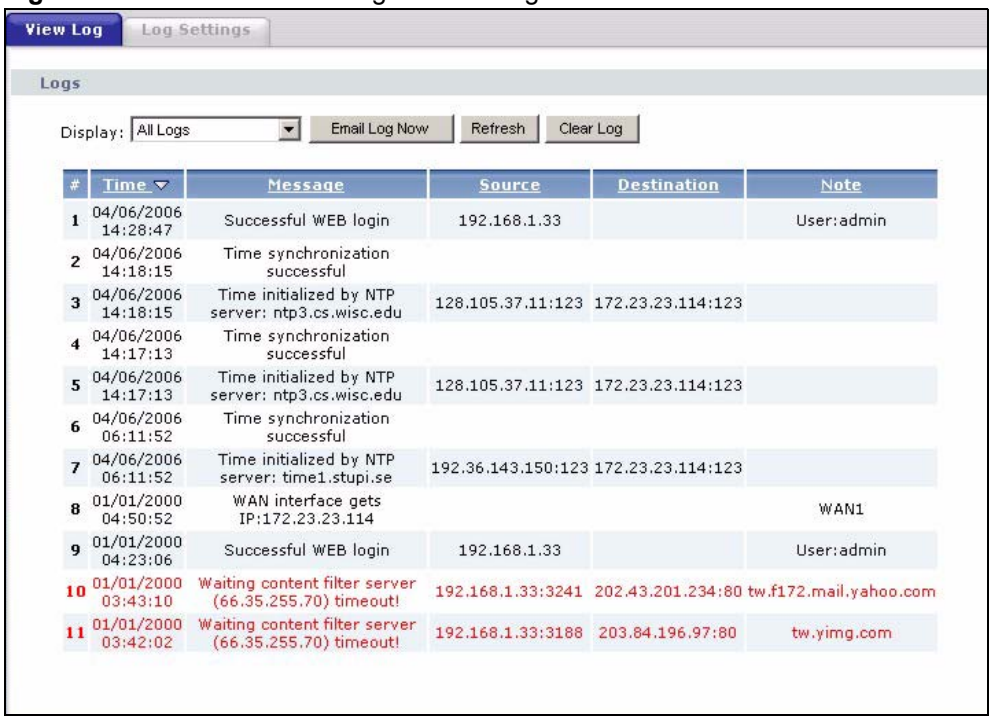
The web configurator allows you to look at all of the NBG420N's logs in one location.

Click **Maintenance** > **Logs** to open the **View Log** screen.

Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 21.2 on page 234). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, Java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 147 Maintenance > Logs > View Log



#	Time	Message	Source	Destination	Note
1	04/06/2006 14:28:47	Successful WEB login	192.168.1.33		User:admin
2	04/06/2006 14:18:15	Time synchronization successful			
3	04/06/2006 14:18:15	Time initialized by NTP server: ntp3.cs.wisc.edu	128.105.37.11:123	172.23.23.114:123	
4	04/06/2006 14:17:13	Time synchronization successful			
5	04/06/2006 14:17:13	Time initialized by NTP server: ntp3.cs.wisc.edu	128.105.37.11:123	172.23.23.114:123	
6	04/06/2006 06:11:52	Time synchronization successful			
7	04/06/2006 06:11:52	Time initialized by NTP server: time1.stupi.se	192.36.143.150:123	172.23.23.114:123	
8	01/01/2000 04:50:52	WAN interface gets IP:172.23.23.114			WAN1
9	01/01/2000 04:23:06	Successful WEB login	192.168.1.33		User:admin
10	01/01/2000 03:43:10	Waiting content filter server (66.35.255.70) timeout!	192.168.1.33:3241	202.43.201.234:80	tw.f172.mail.yahoo.com
11	01/01/2000 03:42:02	Waiting content filter server (66.35.255.70) timeout!	192.168.1.33:3188	203.84.196.97:80	tw.yimg.com

The following table describes the labels in this screen.

Table 86 Maintenance > Logs > View Log

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** page (see Section 21.2 on page 234) display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **Address Info** fields in **Log Settings**).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the NBG420N's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.

21.2 Log Settings

You can configure the NBG420N's general log settings in one location.

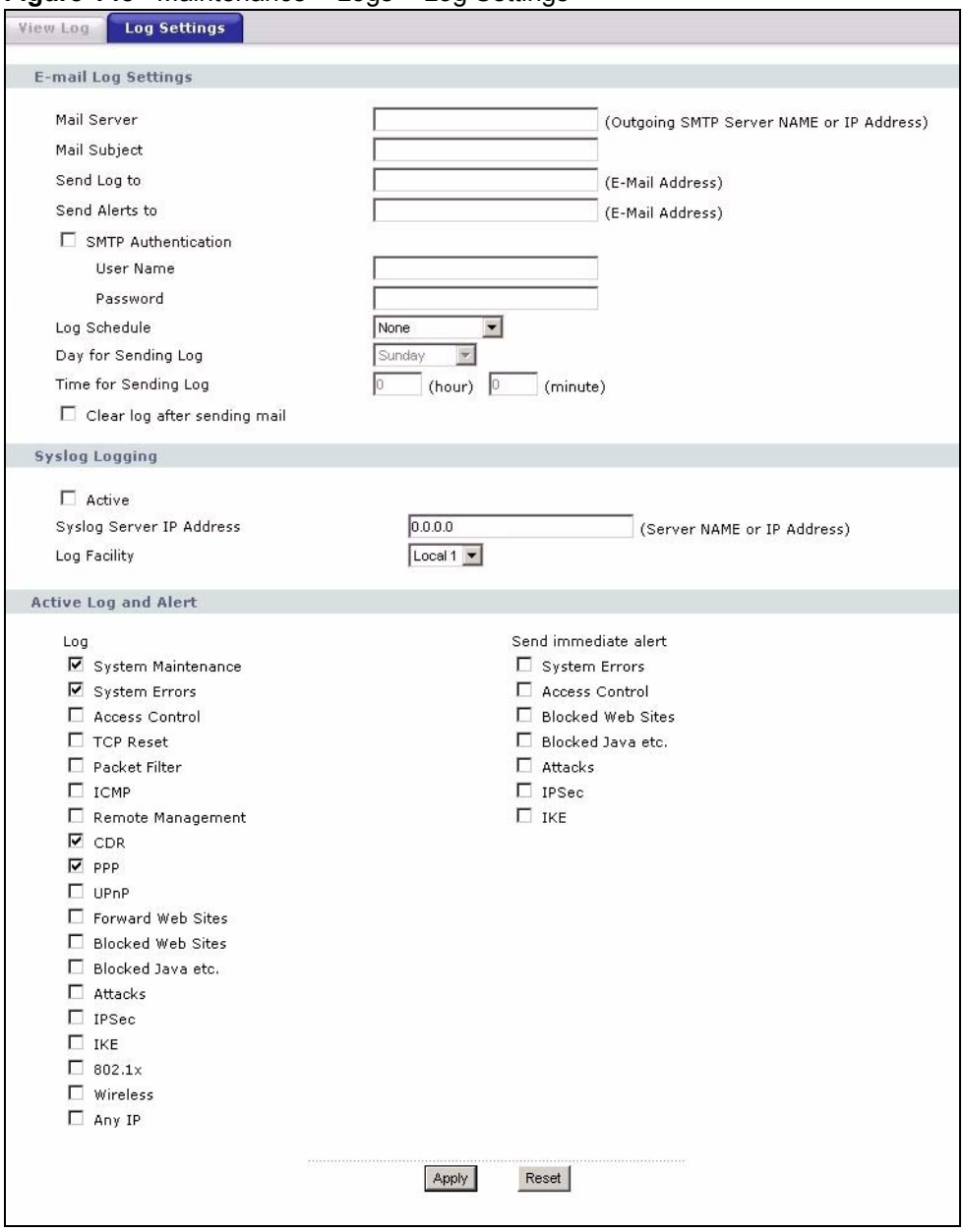
Click **Maintenance** > **Logs** > **Log Settings** to open the **Log Settings** screen.

Use the **Log Settings** screen to configure to where the NBG420N is to send logs; the schedule for when the NBG420N is to send the logs and which logs and/or immediate alerts the NBG420N to send.

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

Figure 148 Maintenance > Logs > Log Settings



The following table describes the labels in this screen.

Table 87 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the NBG420N sends. Not all NBG420N models have this field.
Send Log To	The NBG420N sends logs to the e-mail address specified in this field. If this field is left blank, the NBG420N does not send logs via e-mail.

Table 87 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Send Alerts To	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.
User Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • Daily • Weekly • Hourly • When Log is Full • None. If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the checkbox to delete all the logs after the NBG420N sends an E-mail of the logs.
Syslog Logging	The NBG420N sends a log to an external syslog server.
Active	Click **Active** to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the NBG420N to send E-mail alerts immediately.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

21.3 Log Descriptions

This section provides descriptions of example log messages.

Table 88 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The router has adjusted its time based on information from the time server.
Time calibration failed	The router failed to get information from the time server.
WAN interface gets IP:%s	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns%s	The DHCP server assigned an IP address to a client.
Successful WEB login	Someone has logged on to the router's web configurator interface.
WEB login failed	Someone has failed to log on to the router's web configurator interface.
Successful TELNET login	Someone has logged on to the router via telnet.
TELNET login failed	Someone has failed to log on to the router via telnet.
Successful FTP login	Someone has logged on to the router via ftp.
FTP login failed	Someone has failed to log on to the router via ftp.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
Starting Connectivity Monitor	Starting Connectivity Monitor.
Time initialized by Daytime Server	The router got the time and date from the Daytime server.
Time initialized by Time server	The router got the time and date from the time server.
Time initialized by NTP server	The router got the time and date from the NTP server.
Connect to Daytime server fail	The router was not able to connect to the Daytime server.
Connect to Time server fail	The router was not able to connect to the Time server.
Connect to NTP server fail	The router was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The router dropped an ICMP packet that was too large.
Configuration Change: PC = 0x%x, Task ID = 0x%x	The router is saving configuration changes.
Successful SSH login	Someone has logged on to the router’s SSH server.
SSH login failed	Someone has failed to log on to the router’s SSH server.
Successful HTTPS login	Someone has logged on to the router's web configurator interface using HTTPS protocol.
HTTPS login failed	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.

Table 89 System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
setNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
readNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
WAN connection is down.	A WAN connection is down. You cannot access the network through this interface.

Table 90 Access Control Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: [TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]	The router blocked a packet that didn't have a corresponding NAT table entry.
Router sent blocked web site message: TCP	The router sent a message to notify a user that the router blocked access to a web site that the user requested.

Table 91 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen.
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.

Table 91 TCP Reset Logs (continued)

LOG MESSAGE	DESCRIPTION
`Firewall session time out, sent TCP RST`	The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds
`Exceed MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > “Maximum Incomplete High”, the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < “Maximum Incomplete Low”.
`Access block, sent TCP RST`	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: "sys firewall tcprst").

Table 92 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
`[TCP | UDP | ICMP | IGMP | Generic] packet filter matched (set:%d, rule:%d)`	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

Table 93 ICMP Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>`	ICMP access matched the default policy and was blocked or forwarded according to the user's setting. For type and code details, see Table 104 on page 247.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	ICMP access matched (or didn’t match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule. For type and code details, see Table 104 on page 247.
`Triangle route packet forwarded: ICMP`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: ICMP`	The router blocked a packet that didn’t have a corresponding NAT table entry.
`Unsupported/out-of-order ICMP: ICMP`	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
`Router reply ICMP packet: ICMP`	The router sent an ICMP reply packet to the sender.

Table 94 CDR Logs

LOG MESSAGE	DESCRIPTION
board%d line%d channel%d, call%d,%s C01 Outgoing Call dev=%x ch=%x%s	The router received the setup requirements for a call. “call” is the reference (count) number of the call. “dev” is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or “ch” is the call channel ID.For example,"board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times.
board%d line%d channel%d, call%d,%s C02 OutCall Connected%d%s	The PPPoE, PPTP or dial-up call is connected.
board%d line%d channel%d, call%d,%s C02 Call Terminated	The PPPoE, PPTP or dial-up call was disconnected.

Table 95 PPP Logs

LOG MESSAGE	DESCRIPTION
ppp:LCP Starting	The PPP connection’s Link Control Protocol stage has started.
ppp:LCP Opening	The PPP connection’s Link Control Protocol stage is opening.
ppp:CHAP Opening	The PPP connection’s Challenge Handshake Authentication Protocol stage is opening.
ppp:IPCP Starting	The PPP connection’s Internet Protocol Control Protocol stage is starting.
ppp:IPCP Opening	The PPP connection’s Internet Protocol Control Protocol stage is opening.
ppp:LCP Closing	The PPP connection’s Link Control Protocol stage is closing.
ppp:IPCP Closing	The PPP connection’s Internet Protocol Control Protocol stage is closing.

Table 96 UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 97 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: Keyword blocking	The content of a requested web page matched a user defined keyword.
%s: Not in trusted web list	The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites.
%s: Forbidden Web site	The web site is in the forbidden web site list.
%s: Contains ActiveX	The web site contains ActiveX.
%s: Contains Java applet	The web site contains a Java applet.
%s: Contains cookie	The web site contains a cookie.

Table 97 Content Filtering Logs (continued)

LOG MESSAGE	DESCRIPTION
%s: Proxy mode detected	The router detected proxy mode in the packet.
%s	The content filter server responded that the web site is in the blocked category list, but it did not return the category type.
%s:%s	The content filter server responded that the web site is in the blocked category list, and returned the category type.
%s(cache hit)	The system detected that the web site is in the blocked list from the local cache, but does not know the category type.
%s:%s(cache hit)	The system detected that the web site is in blocked list from the local cache, and knows the category type.
%s: Trusted Web site	The web site is in a trusted domain.
%s	When the content filter is not on according to the time schedule or you didn't select the "Block Matched Web Site" check box, the system forwards the web content.
Waiting content filter server timeout	The external content filtering server did not respond within the timeout period.
DNS resolving failed	The NBG420N cannot get the IP address of the external content filtering via DNS query.
Creating socket failed	The NBG420N cannot issue a query because TCP/IP socket creation failed, port:port number.
Connecting to content filter server fail	The connection to the external content filtering server failed.
License key is invalid	The external content filtering license key is invalid.

Table 98 Attack Logs

LOG MESSAGE	DESCRIPTION
attack [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack. For type and code details, see Table 104 on page 247.
land [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack. For type and code details, see Table 104 on page 247.
ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port. For type and code details, see Table 104 on page 247.
icmp echo: ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack. For type and code details, see Table 104 on page 247.
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.

Table 98 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack. For type and code details, see Table 104 on page 247.
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]	The firewall classified a packet with no source routing entry as an IP spoofing attack.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack. For type and code details, see Table 104 on page 247.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack. For type and code details, see Table 104 on page 247.

Table 99 IPSec Logs

LOG MESSAGE	DESCRIPTION
Discard REPLAY packet	The router received and discarded a packet with an incorrect sequence number.
Inbound packet authentication failed	The router received a packet that has been altered. A third party may have altered or tampered with the packet.
Receive IPSec packet, but no corresponding tunnel exists	The router dropped an inbound packet for which SPI could not find a corresponding phase 2 SA.
Rule <%d> idle time out, disconnect	The router dropped a connection that had outbound traffic and no inbound traffic for a certain time period. You can use the "ipsec timer chk_conn" CI command to set the time period. The default value is 2 minutes.
WAN IP changed to <IP>	The router dropped all connections with the “MyIP” configured as “0.0.0.0” when the WAN IP address changed.

Table 100 IKE Logs

LOG MESSAGE	DESCRIPTION
Active connection allowed exceeded	The IKE process for a new connection failed because the limit of simultaneous phase 2 SAs has been reached.
Start Phase 2: Quick Mode	Phase 2 Quick Mode has started.
Verifying Remote ID failed:	The connection failed during IKE phase 2 because the router and the peer’s Local/Remote Addresses don’t match.

Table 100 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Verifying Local ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
IKE Packet Retransmit	The router retransmitted the last packet sent because there was no response from the peer.
Failed to send IKE Packet	An Ethernet error stopped the router from sending IKE packets.
Too many errors! Deleting SA	An SA was deleted because there were too many errors.
Phase 1 IKE SA process done	The phase 1 IKE SA process has been completed.
Duplicate requests with the same cookie	The router received multiple requests from the same peer while still processing the first IKE packet from the peer.
IKE Negotiation is in process	The router has already started negotiating with the peer for the connection, but the IKE process has not finished yet.
No proposal chosen	Phase 1 or phase 2 parameters don't match. Please check all protocols / settings. Ex. One device being configured for 3DES and the other being configured for DES causes the connection to fail.
Local / remote IPs of incoming request conflict with rule <%d>	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
Cannot resolve Secure Gateway Addr for rule <%d>	The router couldn't resolve the IP address from the domain name that was used for the secure gateway address.
Peer ID: <peer id> <My remote type> -<My local type>	The displayed ID information did not match between the two ends of the connection.
vs. My Remote <My remote> - <My remote>	The displayed ID information did not match between the two ends of the connection.
vs. My Local <My local>-<My local>	The displayed ID information did not match between the two ends of the connection.
Send <packet>	A packet was sent.
Recv <packet>	IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the LOG. Refer to RFC2408 – ISAKMP for a list of all ISAKMP payload types.
Recv <Main or Aggressive> Mode request from <IP>	The router received an IKE negotiation request from the peer address specified.
Send <Main or Aggressive> Mode request to <IP>	The router started negotiation with the peer.
Invalid IP <Peer local> / <Peer local>	The peer's "Local IP Address" is invalid.
Remote IP <Remote IP> / <Remote IP> conflicts	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
Phase 1 ID type mismatch	This router's "Peer ID Type" is different from the peer IPSec router's "Local ID Type".
Phase 1 ID content mismatch	This router's "Peer ID Content" is different from the peer IPSec router's "Local ID Content".

Table 100 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
No known phase 1 ID type found	The router could not find a known phase 1 ID in the connection attempt.
ID type mismatch. Local / Peer: <Local ID type/Peer ID type>	The phase 1 ID types do not match.
ID content mismatch	The phase 1 ID contents do not match.
Configured Peer ID Content: <Configured Peer ID Content>	The phase 1 ID contents do not match and the configured "Peer ID Content" is displayed.
Incoming ID Content: <Incoming Peer ID Content>	The phase 1 ID contents do not match and the incoming packet's ID content is displayed.
Unsupported local ID Type: <%d>	The phase 1 ID type is not supported by the router.
Build Phase 1 ID	The router has started to build the phase 1 ID.
Adjust TCP MSS to%d	The router automatically changed the TCP Maximum Segment Size value after establishing a tunnel.
Rule <%d> input idle time out, disconnect	The tunnel for the listed rule was dropped because there was no inbound traffic within the idle timeout period.
XAUTH succeed! Username: <Username>	The router used extended authentication to authenticate the listed username.
XAUTH fail! Username: <Username>	The router was not able to use extended authentication to authenticate the listed username.
Rule[%d] Phase 1 negotiation mode mismatch	The listed rule's IKE phase 1 negotiation mode did not match between the router and the peer.
Rule [%d] Phase 1 encryption algorithm mismatch	The listed rule's IKE phase 1 encryption algorithm did not match between the router and the peer.
Rule [%d] Phase 1 authentication algorithm mismatch	The listed rule's IKE phase 1 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 1 authentication method mismatch	The listed rule's IKE phase 1 authentication method did not match between the router and the peer.
Rule [%d] Phase 1 key group mismatch	The listed rule's IKE phase 1 key group did not match between the router and the peer.
Rule [%d] Phase 2 protocol mismatch	The listed rule's IKE phase 2 protocol did not match between the router and the peer.
Rule [%d] Phase 2 encryption algorithm mismatch	The listed rule's IKE phase 2 encryption algorithm did not match between the router and the peer.
Rule [%d] Phase 2 authentication algorithm mismatch	The listed rule's IKE phase 2 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 2 encapsulation mismatch	The listed rule's IKE phase 2 encapsulation did not match between the router and the peer.
Rule [%d]> Phase 2 pfs mismatch	The listed rule's IKE phase 2 perfect forward secret (pfs) setting did not match between the router and the peer.

Table 100 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Rule [%d] Phase 1 ID mismatch	The listed rule's IKE phase 1 ID did not match between the router and the peer.
Rule [%d] Phase 1 hash mismatch	The listed rule's IKE phase 1 hash did not match between the router and the peer.
Rule [%d] Phase 1 preshared key mismatch	The listed rule's IKE phase 1 pre-shared key did not match between the router and the peer.
Rule [%d] Tunnel built successfully	The listed rule's IPSec tunnel has been built successfully.
Rule [%d] Peer's public key not found	The listed rule's IKE phase 1 peer's public key was not found.
Rule [%d] Verify peer's signature failed	The listed rule's IKE phase 1verification of the peer's signature failed.
Rule [%d] Sending IKE request	IKE sent an IKE request for the listed rule.
Rule [%d] Receiving IKE request	IKE received an IKE request for the listed rule.
Swap rule to rule [%d]	The router changed to using the listed rule.
Rule [%d] Phase 1 key length mismatch	The listed rule's IKE phase 1 key length (with the AES encryption algorithm) did not match between the router and the peer.
Rule [%d] phase 1 mismatch	The listed rule's IKE phase 1 did not match between the router and the peer.
Rule [%d] phase 2 mismatch	The listed rule's IKE phase 2 did not match between the router and the peer.
Rule [%d] Phase 2 key length mismatch	The listed rule's IKE phase 2 key lengths (with the AES encryption algorithm) did not match between the router and the peer.

Table 101 PKI Logs

LOG MESSAGE	DESCRIPTION
Enrollment successful	The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port.
Enrollment failed	The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
Failed to resolve <SCEP CA server url>	The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved.
Enrollment successful	The CMP online certificate enrollment was successful. The Destination field records the certification authority server's IP address and port.
Enrollment failed	The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
Failed to resolve <CMP CA server url>	The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved.
Rcvd ca cert: <subject name>	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.

Table 101 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
Rcvd user cert: <subject name>	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd CRL <size>: <issuer name>	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd ARL <size>: <issuer name>	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ca cert	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received user cert	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received CRL	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ARL	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.
Rcvd data <size> too large! Max size allowed: <max size>	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
Cert trusted: <subject name>	The router has verified the path of the certificate with the listed subject name.
Due to <reason codes>, cert not trusted: <subject name>	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 104 on page 247 for the corresponding descriptions of the codes.

Table 102 802.1X Logs

LOG MESSAGE	DESCRIPTION
Local User Database accepts user.	A user was authenticated by the local user database.
Local User Database reports user credential error.	A user was not authenticated by the local user database because of an incorrect user password.
Local User Database does not find user`s credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
Local User Database does not support authentication method.	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
User logout because of session timeout expired.	The router logged out a user whose session expired.

Table 102 802.1X Logs (continued)

LOG MESSAGE	DESCRIPTION
`User logout because of user deassociation.`	The router logged out a user who ended the session.
`User logout because of no authentication response from user.`	The router logged out a user from which there was no authentication response.
`User logout because of idle timeout expired.`	The router logged out a user whose idle timeout period expired.
`User logout because of user request.`	A user logged out.
`Local User Database does not support authentication method.`	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
`No response from RADIUS. Pls check RADIUS Server.`	There is no response message from the RADIUS server, please check the RADIUS server.
`Use Local User Database to authenticate user.`	The local user database is operating as the authentication server.
`Use RADIUS to authenticate user.`	The RADIUS server is operating as the authentication server.
`No Server to authenticate user.`	There is no authentication server to authenticate a user.
`Local User Database does not find user`s credential.`	A user was not authenticated by the local user database because the user is not listed in the local user database.

Table 103 ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(L to L/P)	LAN to LAN/ NBG420N	ACL set for packets traveling from the LAN to the LAN or the NBG420N.
(W to W/P)	WAN to WAN/ NBG420N	ACL set for packets traveling from the WAN to the WAN or the NBG420N.

Table 104 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)

Table 104 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 105 Syslog Logs

LOG MESSAGE	DESCRIPTION
<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>	"This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU->LOGS->Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 106 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

22 Tools

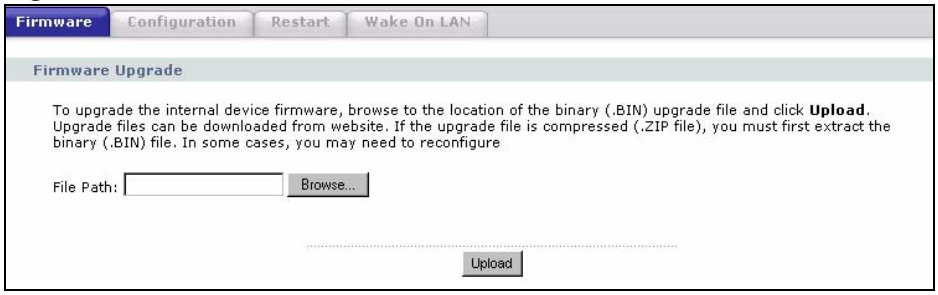
This chapter shows you how to upload a new firmware, upload or save backup configuration files and restart the NBG420N.

22.1 Firmware Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "NBG420N.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Tools**. Follow the instructions in this screen to upload firmware to your NBG420N.

Figure 149 Maintenance > Tools > Firmware


Firmware
Configuration
Restart
Wake On LAN
Firmware Upgrade
To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure
File Path:
Browse...
Upload

The following table describes the labels in this screen.

Table 107 Maintenance > Tools > Firmware

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

Do not turn off the NBG420N while firmware upload is in progress!

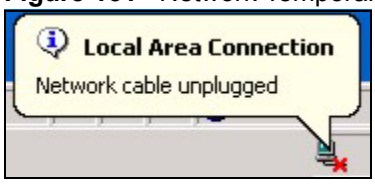
After you see the **Firmware Upload In Process** screen, wait two minutes before logging into the NBG420N again.

Figure 150 Upload Warning

ZyXEL
Firmware Upload In Process
Please Wait ...
Please wait for the device to finish restarting(PWR LED is on steady). This should take about two minutes. To access the device after a successful firmware upload, you need to log in again. Check your new firmware version in the system status menu.

The NBG420N automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 151 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

Figure 152 Upload Error Message

system Upload
Firmware upload error!
The uploaded file was not accepted by the device. Please return to the previous page and select a valid upgrade file. Click Help for more information.
Return

22.2 Configuration Screen

Click **Maintenance > Tools** > **Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 153 Maintenance > Tools > Configuration

Firmware
Configuration
Restart
Wake On LAN
Backup Configuration
Click Backup to save the current configuration of your system to your computer.
Backup
Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
File Path:
Browse...
Upload
Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server
Reset

22.2.1 Backup Configuration

Backup configuration allows you to back up (save) the NBG420N's current configuration to a file on your computer. Once your NBG420N is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the NBG420N's current configuration to your computer.

22.2.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your NBG420N.

Table 108 Maintenance Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Do not turn off the NBG420N while configuration file upload is in progress

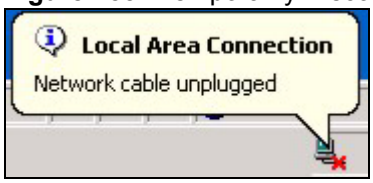
After you see a "configuration upload successful" screen, you must then wait one minute before logging into the NBG420N again.

Figure 154 Configuration Restore Successful

ZyXEL
Restore Configuration successful
The Device Is Rebooting Now.
After the device finishes rebooting, the login screen displays.

The NBG420N automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

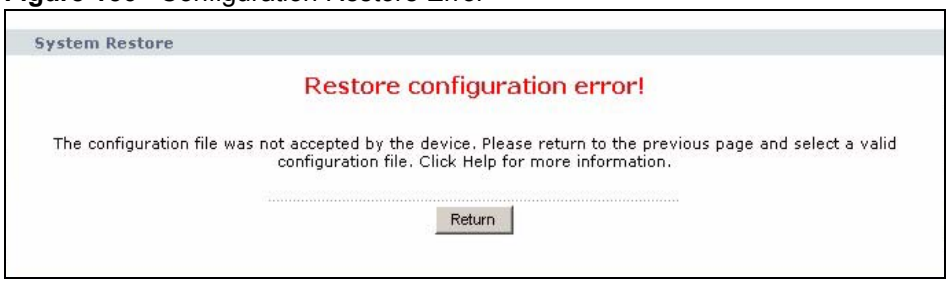
Figure 155 Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default NBG420N IP address (192.168.1.1). See Appendix D on page 293 for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

Figure 156 Configuration Restore Error


System Restore
Restore configuration error!
The configuration file was not accepted by the device. Please return to the previous page and select a valid configuration file. Click Help for more information.
Return

22.2.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the NBG420N to its factory defaults.

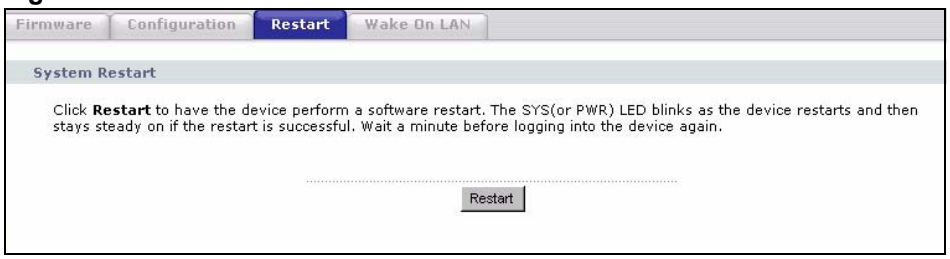
You can also press the **RESET** button on the rear panel to reset the factory defaults of your NBG420N. Refer to the chapter about introducing the web configurator for more information on the **RESET** button.

22.3 Restart Screen

System restart allows you to reboot the NBG420N without turning the power off.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the NBG420N reboot. This does not affect the NBG420N's configuration.

Figure 157 Maintenance > Tools > Restart


Firmware
Configuration
Restart
Wake On LAN
System Restart
Click Restart to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.
Restart

22.4 Wake On LAN

Wake On LAN (WoL) allows you to remotely turn on a device on the network. To use this feature the remote hardware (for example the network adapter on your computer) must support Wake On LAN using the "Magic Packet" method.

You need to know the MAC address of the remote device. It may be on a label on the device or in it's documentation.

Click **Maintenance > Tools** > **Wake On LAN** to use this feature.

The NBG420N can only wake up remote devices that exist in it's ARP table. For the remote device to exist in the NBG420N's ARP table it should have had a prior connection with the NBG420N.

Figure 158 Maintenance > Tools > Wake On LAN

The following table describes the labels in this screen.

Table 109 Maintenance > Tools > Wake On LAN

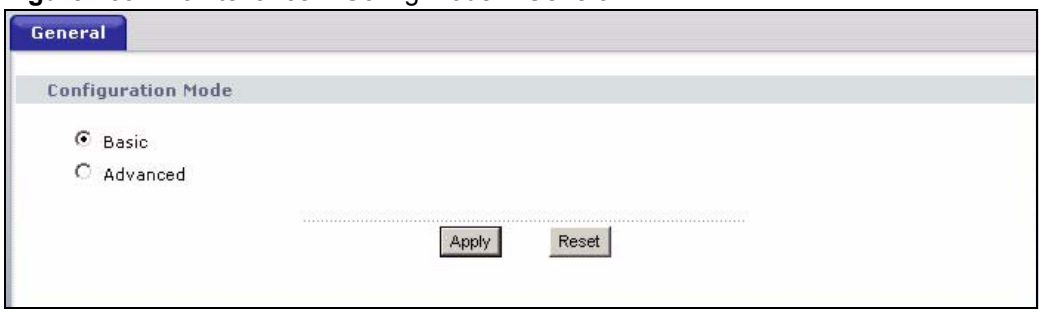
LABEL	DESCRIPTION
Target's MAC Address	Enter the MAC Address of the device on the network that will be turned on. A MAC address consists of six hexadecimal character pairs.
Wake up	Click this to turn the specified device on. The status bar will refresh and indicate either **Ready** or **MAC Address error**. If it displays **Ready** you should check if the remote device has turned on. If the status bar displays **MAC Address error** it means you may have input the MAC Address incorrectly. Make sure you are entering it in the correct format.

23

Configuration Mode

Click **Maintenance > Config Mode** to open the following screen. This screen allows you to hide or display the advanced screens of some features or the advanced features, such as MAC filter or static route. **Basic** is selected by default and you cannot see the advanced screens or features. If you want to view and configure all screens including the advanced ones, select **Advanced** and click **Apply**.

Figure 159 Maintenance > Config Mode > General



The following table describes the labels in the screen.

Table 110 Maintenance > Config Mode > General

LABEL	DESCRIPTION
Configuration Mode	
Basic	Select **Basic** mode to enable or disable features and to monitor the status of your device.
Advanced	Select **Advanced** mode to set advanced settings.
Apply	Click on this to set the mode.
Reset	Click on this to reset your selection.

The following table includes the screens that you can view and configure only when you select **Advanced**.

Table 111 Advanced Configuration Options

CATEGORY	LINK	TAB
Network	Wireless LAN	MAC Filter
		Advanced
		QoS
		Scheduling
	WAN	Advanced
	LAN	IP Alias
		Advanced
	DHCP Server	Advanced
	NAT	Advanced
Security	Firewall	Services
	Content Filter	Schedule
Management	Static Route	IP Static Route
	Bandwidth MGMT	Advanced
		Monitor
	Remote MGMT	Telnet
		FTP
		DNS
Maintenance	Logs	Log Settings

In **AP Mode** many screens will not be available. See Chapter 5 on page 65 for more information.

24

Sys Op Mode

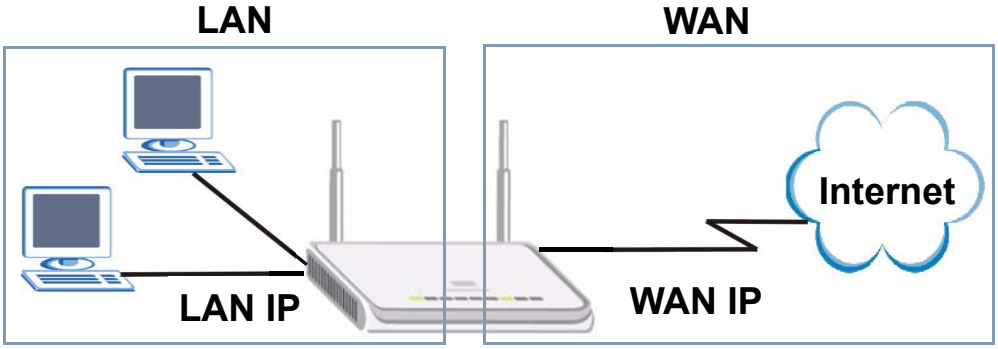
24.1 Overview

The **Sys Op Mode** (System Operation Mode) function lets you configure whether your NBG420N is a router or AP. You can choose between **Router Mode** and **AP Mode** depending on your network topology and the features you require from your device. See Section 1.1 on page 31 for more information on which mode to choose.

24.1.1 Router

A router connects your local network with another network, such as the Internet. The router has two IP addresses, the LAN IP address and the WAN IP address.

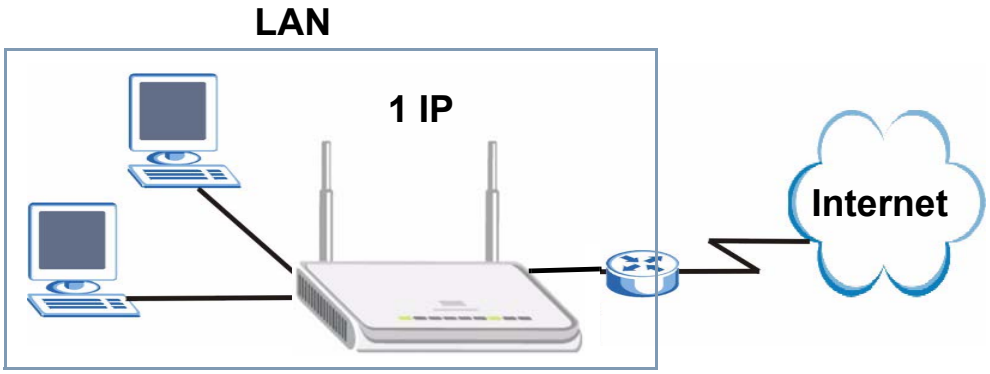
Figure 160 LAN and WAN IP Addresses in Router Mode



24.1.2 AP

An AP extends one network and so has just one IP address. All Ethernet ports on the AP have the same IP address. To connect to the Internet, another device, such as a router, is required.

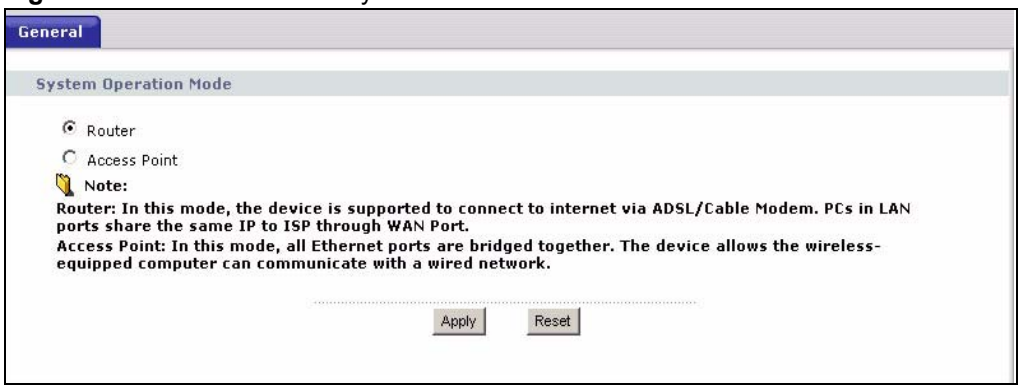
Figure 161 IP Address in AP Mode



24.2 Selecting System Operation Mode

Use this screen to select how you connect to the Internet.

Figure 162 Maintenance > Sys OP Mode > General


General
System Operation Mode
Router
Access Point
Note:
Router: In this mode, the device is supported to connect to internet via ADSL/Cable Modem. PCs in LAN ports share the same IP to ISP through WAN Port.
Access Point: In this mode, all Ethernet ports are bridged together. The device allows the wireless-equipped computer can communicate with a wired network.
Apply
Reset

If you select Router Mode, the following pop-up message window appears.

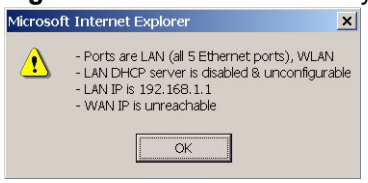
Figure 163 Maintenance > Sys Op Mode > General: Router

Microsoft Internet Explorer
- Ports are LAN (4 Ethernet LAN ports), WLAN, WAN
- LAN DHCP server is configurable
- LAN IP is 192.168.1.1
- WAN IP is configurable
OK

- In this mode there are both LAN and WAN ports. The LAN Ethernet and WAN Ethernet ports have different IP addresses.
- The DHCP server on your device is enabled and allocates IP addresses to other devices on your local network.
- The LAN IP address of the device on the local network is set to 192.168.1.1.
- You can configure the IP address settings on your WAN port. Contact your ISP or system administrator for more information on appropriate settings.

If you select Access Point the following pop-up message window appears.

Figure 164 Maintenance > Sys Op Mode > General: AP


Microsoft Internet Explorer
- Ports are LAN (all 5 Ethernet ports), WLAN
- LAN DHCP server is disabled & unconfigurable
- LAN IP is 192.168.1.1
- WAN IP is unreachable
OK

- In **AP Mode** all Ethernet ports have the same IP address.
- All ports on the rear panel of the device are LAN ports, including the port labeled WAN. There is no WAN port.
- The DHCP server on your device is disabled. In AP mode there must be a device with a DHCP server on your network such as a router or gateway which can allocate IP addresses.

The IP address of the device on the local network is set to 192.168.1.1.

The following table describes the labels in the **General** screen.

Table 112 Maintenance > Sys OP Mode > General

LABEL	DESCRIPTION
System Operation Mode	
Router	Select **Router** if your device routes traffic between a local network and another network such as the Internet. This mode offers services such as a firewall or bandwidth management.
Access Point	Select **Access Point** if your device bridges traffic between clients on the same network.
Apply	Click **Apply** to save your settings.
Reset	Click **Reset** to return your settings to the default (**Router**)

If you select the incorrect System Operation Mode you cannot connect to the Internet.

25

Language

Use this screen to change the language for the web configurator display.

25.1 Language Screen

Click the language you prefer. The web configurator language changes after a while without restarting the NBG420N.

Figure 165 Language

26

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- NBG420N Access and Login
- Internet Access
- Resetting the NBG420N to Its Factory Defaults
- Wireless Router/AP Troubleshooting
- Advanced Features

26.1 Power, Hardware Connections, and LEDs

The NBG420N does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the NBG420N.
2. Make sure the power adaptor or cord is connected to the NBG420N and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the NBG420N.
4. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.7 on page 33.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Disconnect and re-connect the power adaptor to the NBG420N.
5. If the problem continues, contact the vendor.

26.2 NBG420N Access and Login

I don't know the IP address of my NBG420N.

1. The default IP address is **192.168.1.1**.
2. If you changed the IP address and have forgotten it, you might get the IP address of the NBG420N by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the NBG420N (it depends on the network), so enter this IP address in your Internet browser.Set your device to **Router Mode**, login (see the Quick Start Guide for instructions) and go to the **Device Information** table in the **Status** screen. Your NBG420N's IP address is available in the **Device Information** table.
   - If the **DHCP** setting under **LAN information** is **None**, your device has a fixed IP address.
   - If the **DHCP** setting under **LAN information** is **Client**, then your device receives an IP address from a DHCP server on the network.
3. If your NBG420N is a DHCP client, you can find your IP address from the DHCP server. This information is only available from the DHCP server which allocates IP addresses on your network. Find this information directly from the DHCP server or contact your system administrator for more information.
4. Reset your NBG420N to change all settings back to their default. This means your current settings are lost. See Section 26.4 on page 269 in the **Troubleshooting** for information on resetting your NBG420N.

I forgot the password.

1. The default password is **1234**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 26.4 on page 269.

I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.1.
   - If you changed the IP address (Section 7.3 on page 102), use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I don't know the IP address of my NBG420N.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix B on page 279.
4 Make sure your computer is in the same subnet as the NBG420N. (If you know that there are routers between your computer and the NBG420N, skip this step.)
   - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Section 7.3 on page 102.
   - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the NBG420N. See Section 7.3 on page 102.
5 Reset the device to its factory defaults, and try to access the NBG420N with the default IP address. See Section 7.3 on page 102.
6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the NBG420N using another service, such as Telnet. If you can access the NBG420N, check the remote management settings and firewall rules to find out why the NBG420N does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN/ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the NBG420N.

1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.
2 You cannot log in to the web configurator while someone is using Telnet to access the NBG420N. Log out of the NBG420N in the other session, or ask the person who is logged in to log out.
3 Disconnect and re-connect the power adaptor or cord to the NBG420N.
4 If this does not work, you have to reset the device to its factory defaults. See Section 26.4 on page 269.

I cannot Telnet to the NBG420N.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

26.3 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
2. Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
4. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
5. Go to Maintenance > Sys OP Mode > General. Check your System Operation Mode setting.
   - Select **Router** if your device routes traffic between a local network and another network such as the Internet.
   - Select **Access Point** if your device bridges traffic between clients on the same network.
6. If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the NBG420N), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.7 on page 33.
2. Reboot the NBG420N.
3. If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.7 on page 33. If the NBG420N is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength. If the signal strength is low, try moving the NBG420N closer to the AP if possible, and look around to see if there are any devices that might be

interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

3. Reboot the NBG420N.
4. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for bandwidth management. If it is disabled, you might consider activating it. If it is enabled, you might consider changing the allocations.
- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

26.4 Resetting the NBG420N to Its Factory Defaults

If you reset the NBG420N, you lose all of the changes you have made. The NBG420N re-loads its default settings, and the password resets to **1234**. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

To reset the NBG420N,

1. Make sure the power **LED** is on and not blinking.
2. Press and hold the **RESET** button for five to ten seconds. Release the **RESET** button when the power LED begins to blink. The default settings have been restored.

If the NBG420N restarts automatically, wait for the NBG420N to finish restarting, and log in to the web configurator. The password is “1234”.

If the NBG420N does not restart automatically, disconnect and reconnect the NBG420N’s power. Then, follow the directions above again.

26.5 Wireless Router/AP Troubleshooting

I cannot access the NBG420N or ping any computer from the WLAN (wireless AP or router).

1. Make sure the wireless LAN is enabled on the NBG420N
2. Make sure the wireless adapter on the wireless station is working properly.
3. Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the NBG420N.

4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the NBG420N.
5 Check that both the NBG420N and your wireless station are using the same wireless and wireless security settings.
6 Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the NBG420N.
7 Make sure you allow the NBG420N to be remotely accessed through the WLAN interface. Check your remote management settings.

- See the chapter on Wireless LAN in the User's Guide for more information.

26.6 Advanced Features

I can log in, but I cannot see some of the screens or fields in the Web Configurator.

You may be accessing the Web Configurator in Basic mode. Some screens and fields are available only in Advanced mode. Use the **Maintenance > Config** Mode screen to select Advanced mode.

You may be accessing the Web Configurator in AP Mode. Some screens and fields are available only in Router Mode. Use the **Maintenance > Sys OP Mode** screen to select Router Mode.

I set up URL keyword blocking, but I can still access a website that should be blocked.

Make sure that you select the **Enable URL Keyword Blocking** check box in the Content Filtering screen. Make sure that the keywords that you type are listed in the **Keyword List**.

If a keyword that is listed in the **Keyword List** is not blocked when it is found in a URL, customize the keyword blocking using commands. See the Customizing Keyword Blocking URL Checking section in the Content Filter chapter.

PART VI
Appendices and Index

Product Specifications and Wall-Mounting Instructions (273)
Pop-up Windows, JavaScripts and Java Permissions (279)
IP Addresses and Subnetting (285)
Setting up Your Computer's IP Address (293)
Wireless LANs (309)
Services (321)
Legal Information (325)
Customer Support (329)
Index (335)

A

Product Specifications and Wall-Mounting Instructions

The following tables summarize the NBG420N's hardware and firmware features.

Table 113 Hardware Features

Dimensions (W x D x H)	115 x 162 x 33 mm
Weight	230g
Power Specification	Input: 120~240 AC, 50~60 Hz Output: 12 V DC 1 A
Ethernet ports	Auto-negotiating: 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode. Auto-crossover: Use either crossover or straight-through Ethernet cables.
4-5 Port Switch	A combination of switch and router makes your NBG420N a cost-effective and viable network solution. You can add up to four computers to the NBG420N without the cost of a hub when connecting to the Internet through the WAN port. You can add up to five computers to the NBG420N when you connect to the Internet in AP mode. Add more than four computers to your LAN by using a hub.
LEDs	PWR, LAN1-4, WAN, WLAN, WPS
Reset Button	The reset button is built into the rear panel. Use this button to restore the NBG420N to its factory default settings. Press for 1 second to restart the device. Press for 5 seconds to restore to factory default settings.
WPS button	Press the WPS on two WPS enabled devices within 120 seconds for a security-enabled wireless connection.
Antenna	The NBG420N is equipped with two 1.8dBi (2.4GHz) detachable antennas to provide clear radio transmission and reception on the wireless network.
Operation Environment	Temperature: 0º C ~ 40º C Humidity: 20% ~ 95% RH (Non-condensing)
Storage Environment	Temperature: -20º C ~ 60º C Humidity: 20% ~ 95% RH (Non-condensing)
Distance between the centers of the holes on the device's back.	120 mm
Screw size for wall-mounting	M4 Tap Screw

Table 114 Firmware Features

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.33 to 192.168.1.64
Wireless Interface	Wireless LAN
Default Wireless SSID	Wireless LAN: ZyXEL Wireless LAN when WPS enabled: ZyXEL WPS
Default Wireless IP Address	Wireless LAN: Same as LAN (192.168.1.1)
Default Wireless Subnet Mask	Wireless LAN: Same as LAN (255.255.255.0)
Default Wireless DHCP Pool Size	Wireless LAN: Same as LAN (32 from 192.168.1.33 to 192.168.1.64)
Device Management	Use the web configurator to easily configure the rich range of features on the NBG420N.
Wireless Functionality	Allows IEEE 802.11b and/or IEEE 802.11g and/or IEEE 802.11n wireless clients to connect to the NBG420N wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network. Note: The NBG420N may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the NBG420N. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the NBG420N's configuration and put it back on the NBG420N later if you decide you want to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert a single public IP address to multiple private IP addresses for the computers on your network.
Firewall	You can configure firewall on the NBG420N for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example.
Content Filter	The NBG420N blocks or allows access to web sites that you specify and blocks access to web sites with URLs that contain keywords that you specify. You can define time periods and days during which content filtering is enabled. You can also include or exclude particular computers on your network from content filtering. You can also subscribe to category-based content filtering that allows your NBG420N to check web sites against an external database.

Table 114 Firmware Features

FEATURE	DESCRIPTION
IPSec VPN	This allows you to establish a secure Virtual Private Network (VPN) tunnel to connect with business partners and branch offices using data encryption and the Internet without the expense of leased site-to-site lines. The NBG420N VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.
Bandwidth Management	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Wireless LAN Scheduler	You can schedule the times the Wireless LAN is enabled/disabled.
Time and Date	Get the current time and date from an external server when you turn on your NBG420N. You can also set the time manually. These dates and times are then used in logs.
Port Forwarding	If you have a server (mail or web server for example) on your network, then use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the NBG420N assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP Multicast is used to send traffic to a specific group of computers. The NBG420N supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
IP Alias	IP Alias allows you to subdivide a physical network into logical networks over the same Ethernet interface with the NBG420N itself as the gateway for each subnet.
Logging and Tracing	Use packet tracing and logs for troubleshooting. You can send logs from the NBG420N to an external syslog server.
PPPoE	PPPoE mimics a dial-up Internet access connection.
PPTP Encapsulation	Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The NBG420N supports one PPTP connection at a time.
Universal Plug and Play (UPnP)	The NBG420N can communicate with other UPnP enabled devices in a network.

Table 115 Feature Specifications

FEATURE	SPECIFICATION
Number of Static Routes	8
Number of Port Forwarding Rules	10
Number of NAT Sessions	16000
Number of Address Mapping Rules	10
Number of VPN Tunnels	2
Number of Bandwidth Management Classes	3
Number of DNS Name Server Record Entries	3

The following list, which is not exhaustive, illustrates the standards supported in the NBG420N.

Table 116 Standards Supported

STANDARD	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol.
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1631	IP Network Address Translator (NAT)
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2766	Network Address Translation - Protocol
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11n	
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.11x	Port Based Network Access Control.
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
Microsoft PPTP	MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol)
MBM v2	Media Bandwidth Management v2

Wall-mounting Instructions

Do the following to hang your NBG420N on a wall.

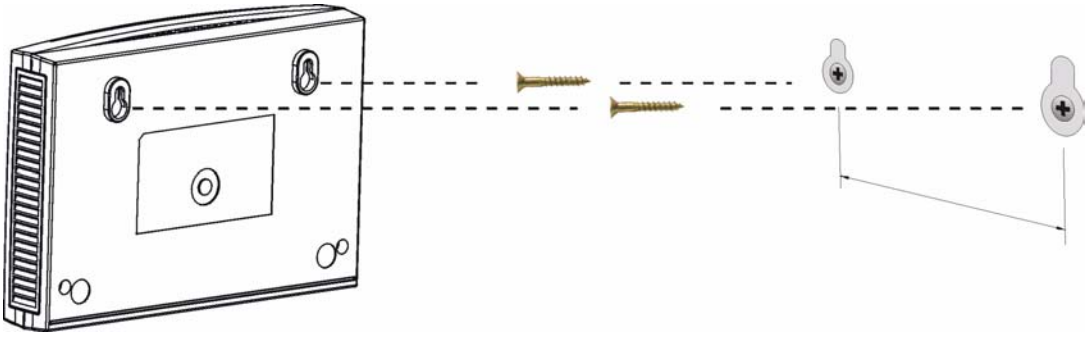
See the Figure 167 on page 278 for the size of screws to use and how far apart to place them.

1. Locate a high position on a wall that is free of obstructions. Use a sturdy wall.
2. Drill two holes for the screws. Make sure the distance between the centers of the holes matches what is listed in the product specifications appendix.

Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

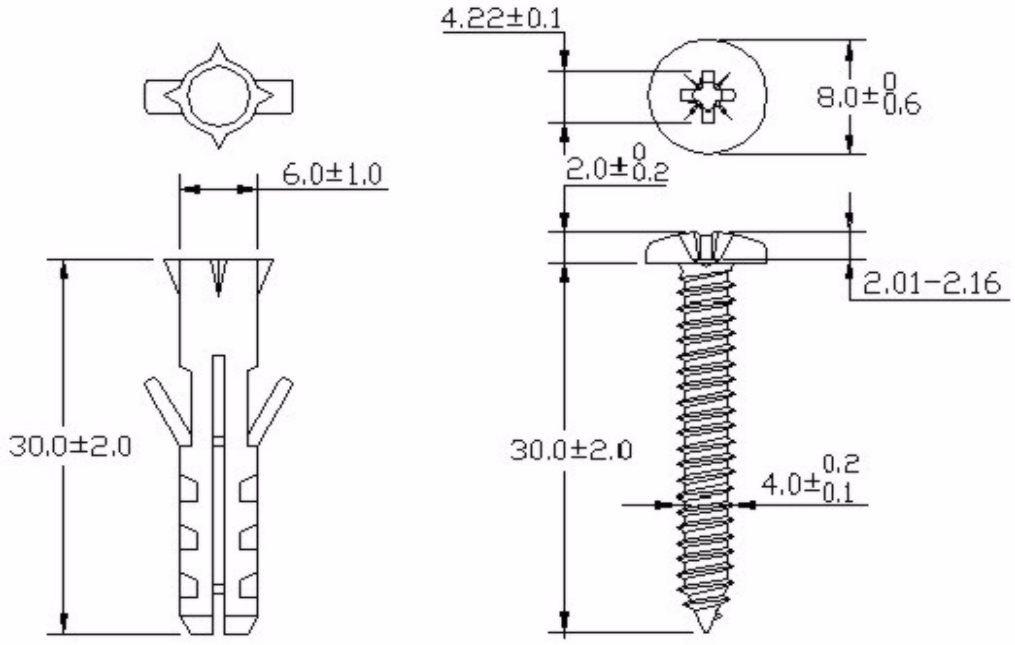
3 Do not screw the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.
4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the NBG420N with the connection cables.
5 Align the holes on the back of the NBG420N with the screws on the wall. Hang the NBG420N on the screws.

Figure 166 Wall-mounting Example



The following are dimensions of an M4 tap screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

Figure 167 Masonry Plug and M4 Tap Screw



B

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

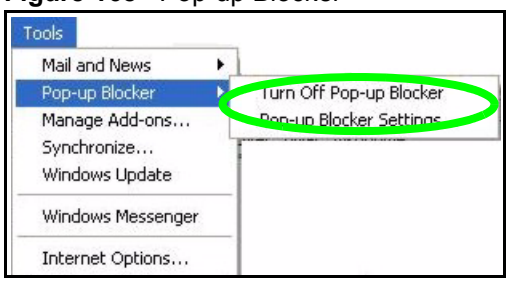
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 168 Pop-up Blocker

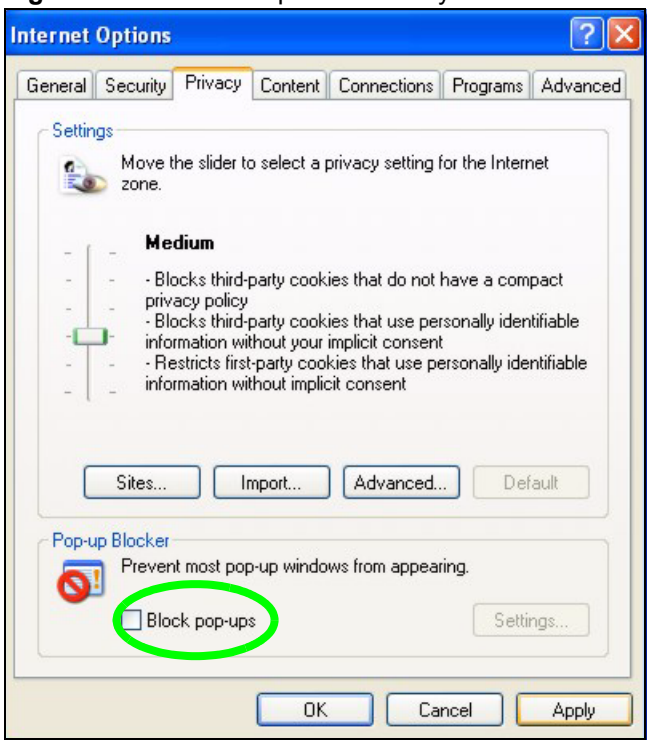


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 169 Internet Options: Privacy



3 Click **Apply** to save this setting.

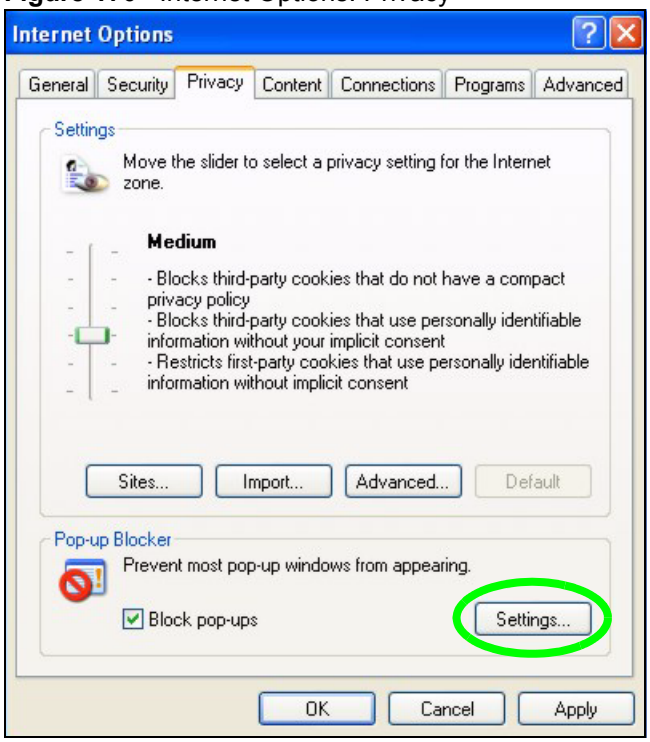
Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

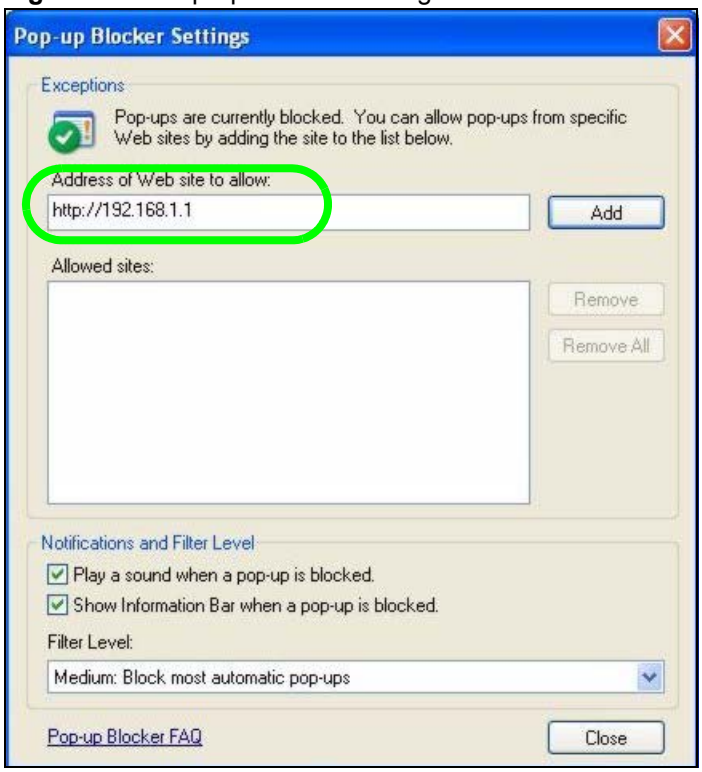
Figure 170 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 171 Pop-up Blocker Settings


Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

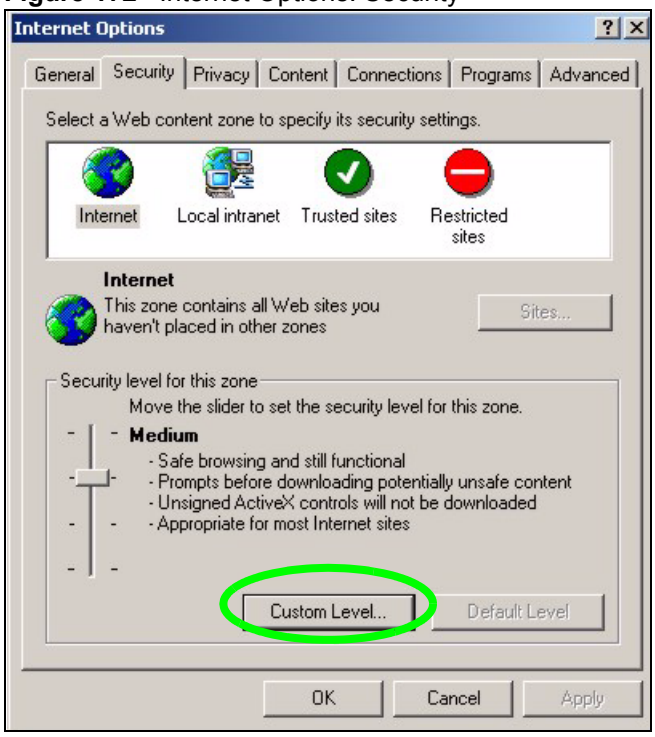
5 Click **Close** to return to the **Privacy** screen.
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

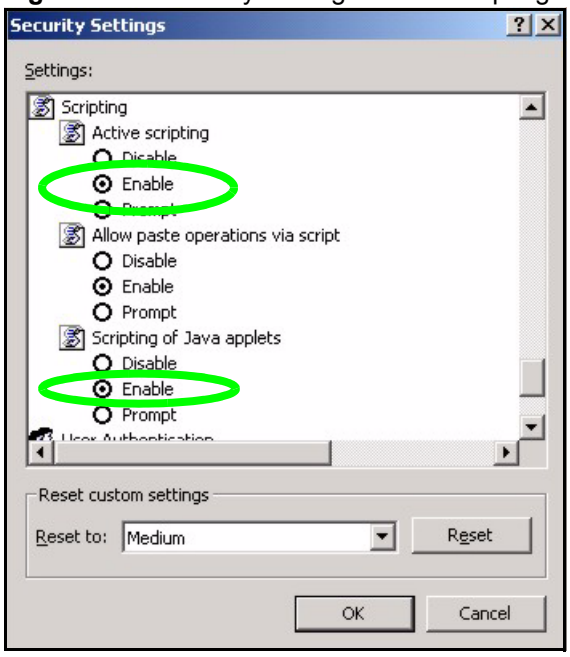
1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 172 Internet Options: Security



2 Click the **Custom Level...** button.
3 Scroll down to **Scripting**.
4 Under **Active scripting** make sure that **Enable** is selected (the default).
5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
6 Click **OK** to close the window.

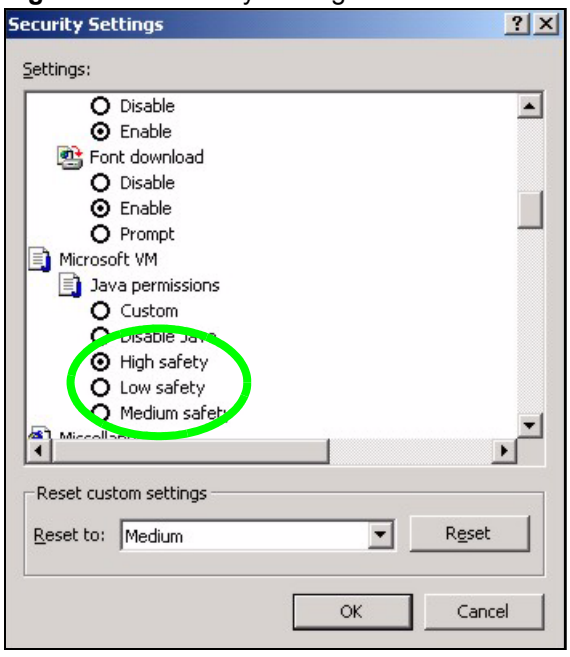
Figure 173 Security Settings - Java Scripting



Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

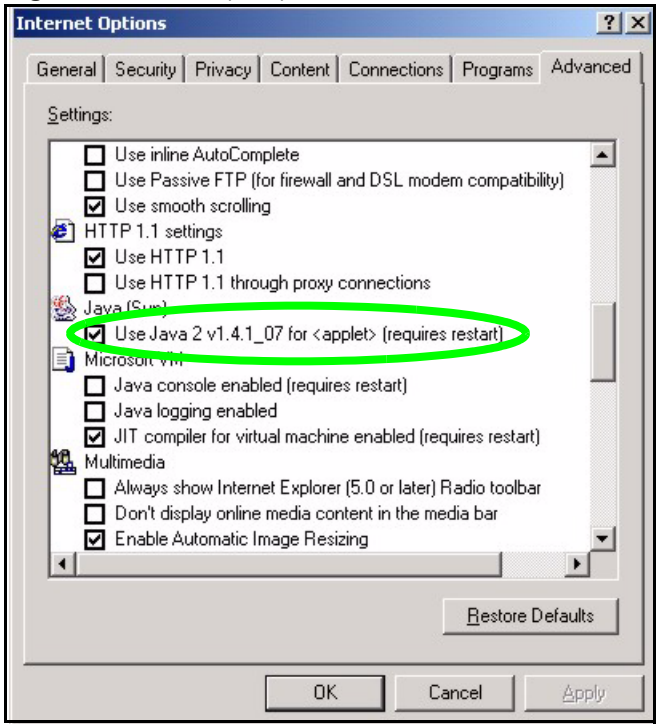
Figure 174 Security Settings - Java



JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.
2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
3 Click **OK** to close the window.

Figure 175 Java (Sun)



C

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

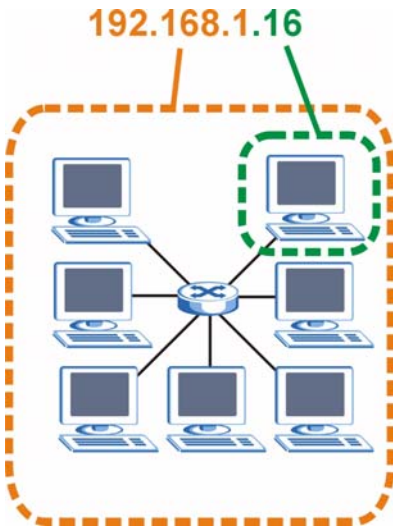
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 176 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 117 Subnet Mask - Identifying Network Number

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 118 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 119 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 120 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 120 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

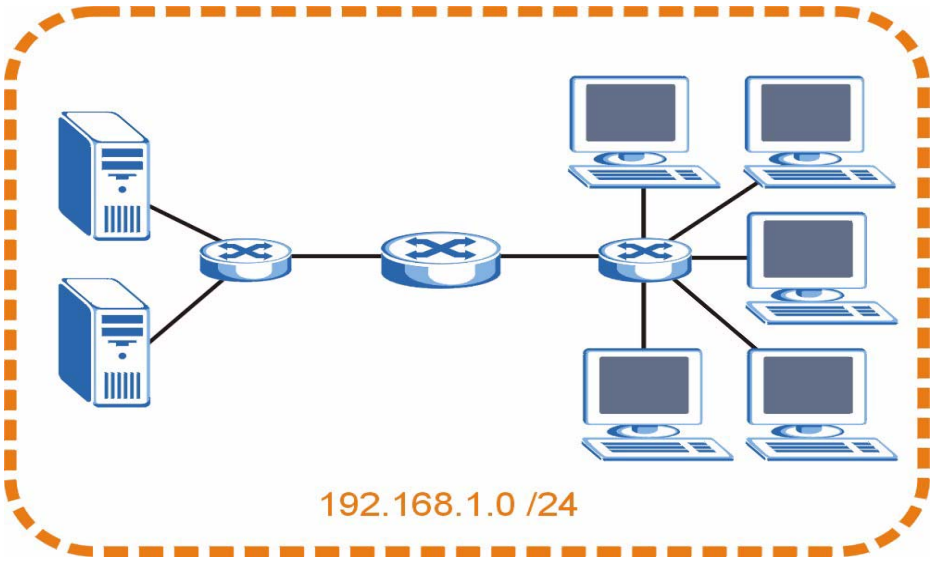
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 177 Subnetting Example: Before Subnetting

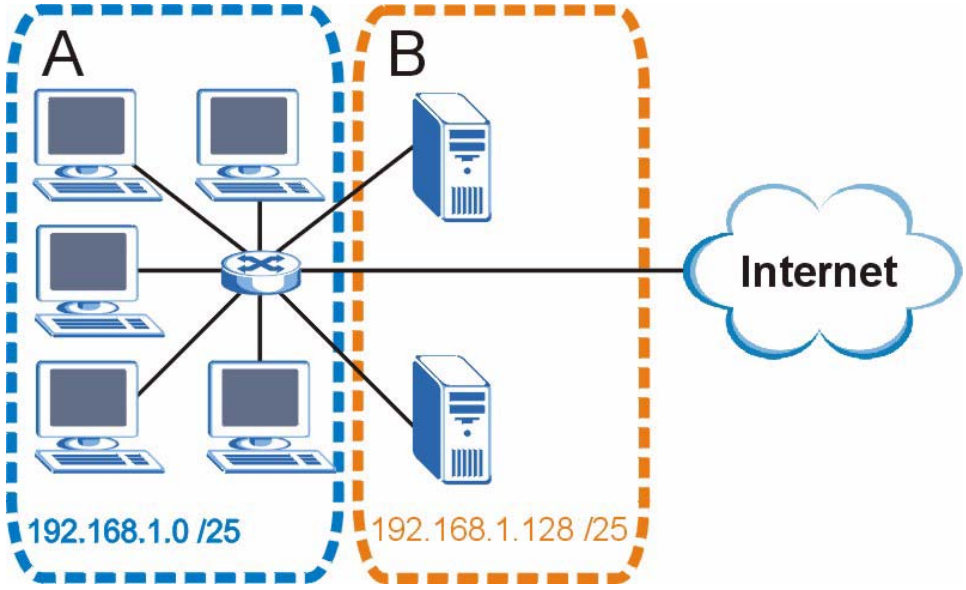


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The "borrowed" host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 178 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 121 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 122 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 123 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 124 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 125 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 125 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 126 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 127 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 127 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the NBG420N.

Once you have decided on the network number, pick an IP address for your NBG420N that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your NBG420N will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the NBG420N unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

D

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

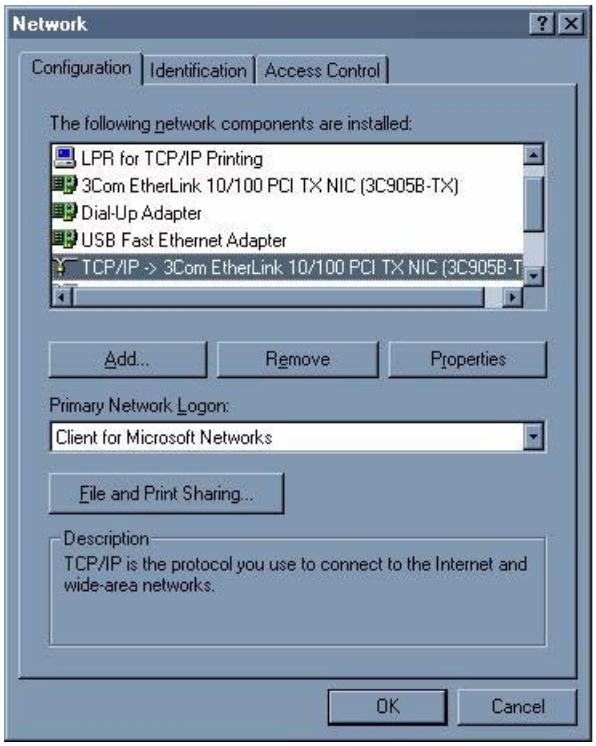
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 179 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

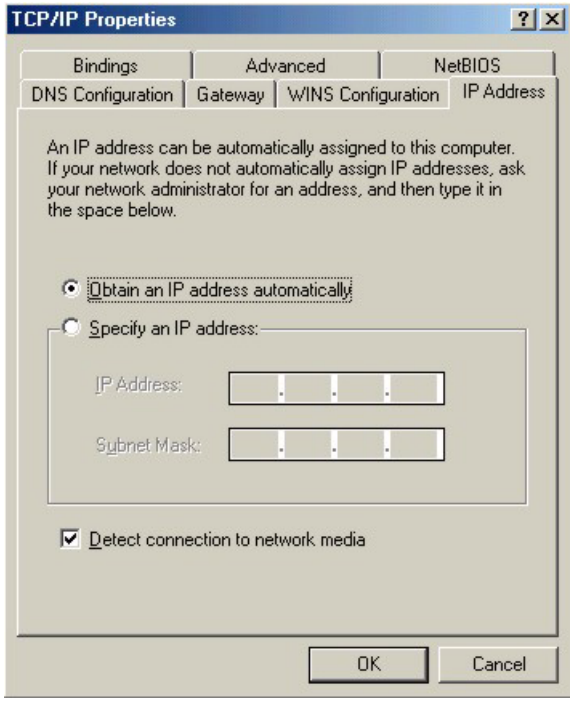
If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.
3. Select **Microsoft** from the list of manufacturers.
4. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
5. Restart your computer so the changes you made take effect.

Configuring

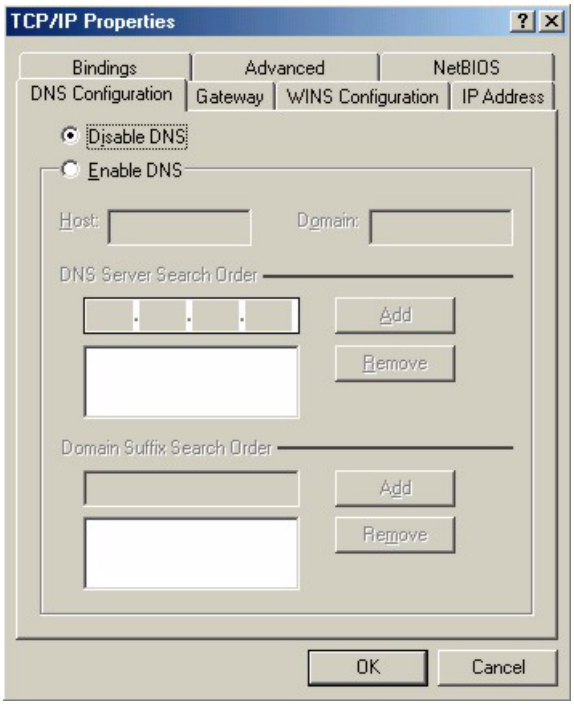
1. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
2. Click the **IP Address** tab.
   - If your IP address is dynamic, select **Obtain an IP address automatically**.
   - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 180 Windows 95/98/Me: TCP/IP Properties: IP Address


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

3. Click the **DNS** Configuration tab.
   - If you do not know your DNS information, select **Disable DNS**.
   - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 181 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.
   - If you do not know your gateway's IP address, remove previously installed gateways.
   - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
5 Click **OK** to save and close the **TCP/IP Properties** window.
6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7 Turn on your Prestige and restart your computer when prompted.

Verifying Settings

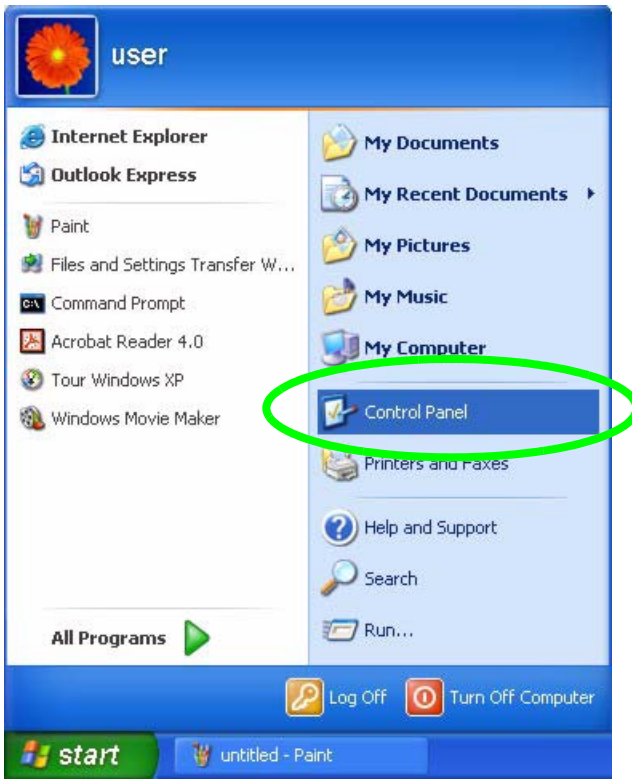
1 Click **Start** and then **Run**.
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 182 Windows XP: Start Menu

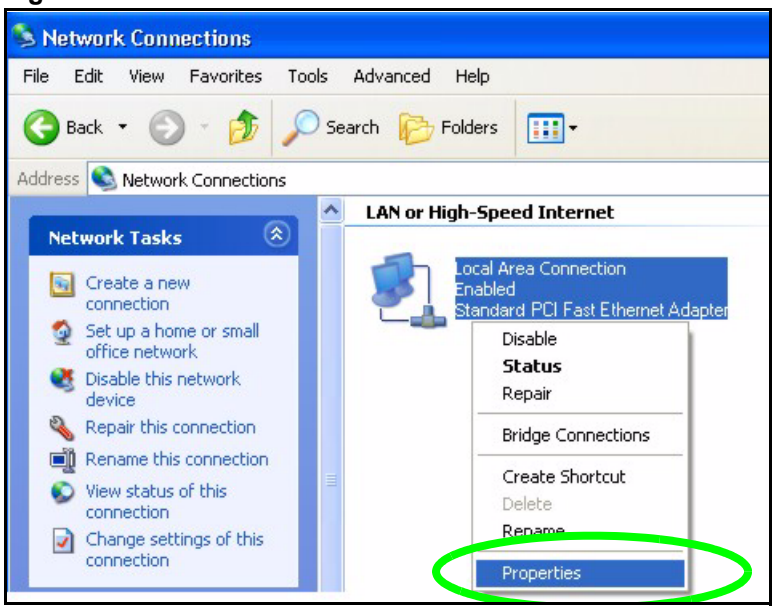


2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 183 Windows XP: Control Panel

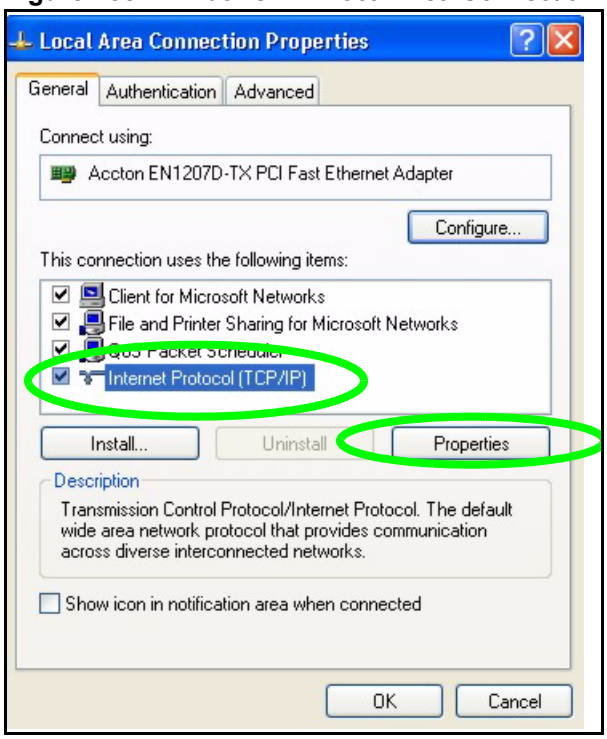
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 184 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

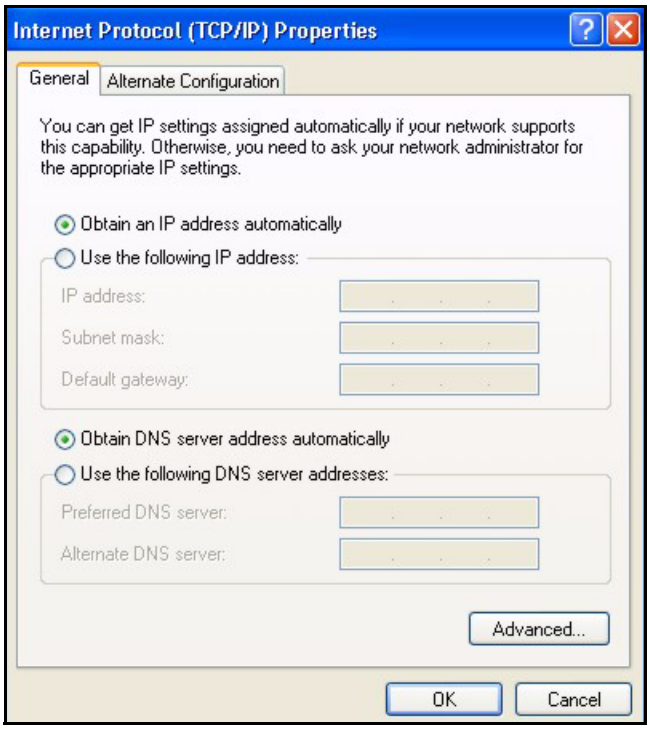
Figure 185 Windows XP: Local Area Connection Properties


Local Area Connection Properties
General Authentication Advanced
Connect using:
Accton EN1207D-TX PCI Fast Ethernet Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 186 Windows XP: Internet Protocol (TCP/IP) Properties

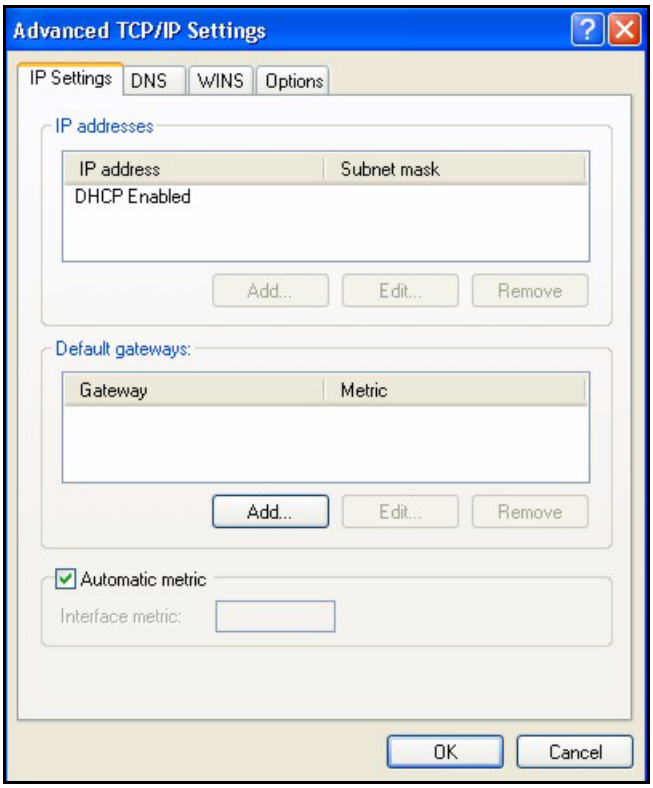

Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 187 Windows XP: Advanced TCP/IP Properties

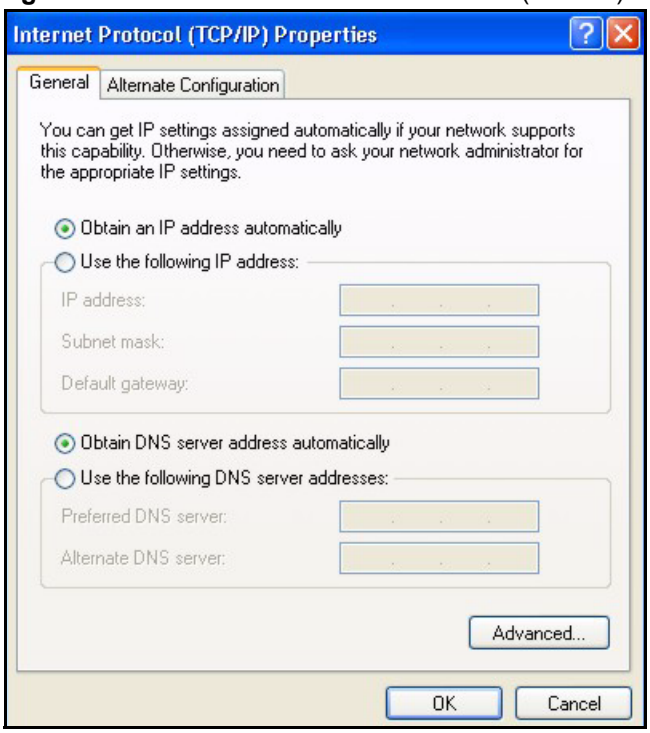


7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 188 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

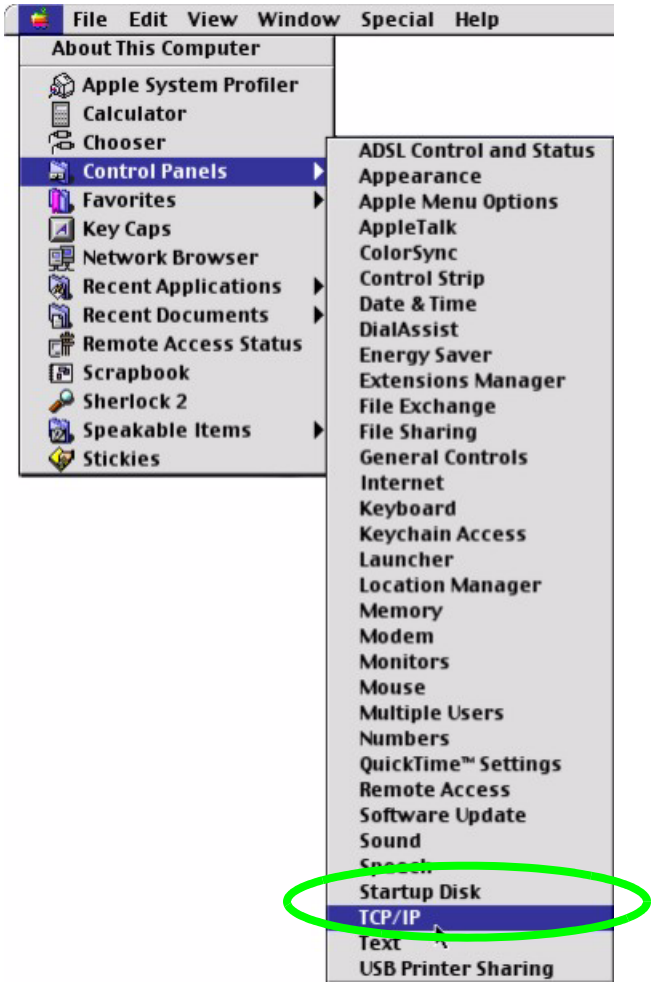
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

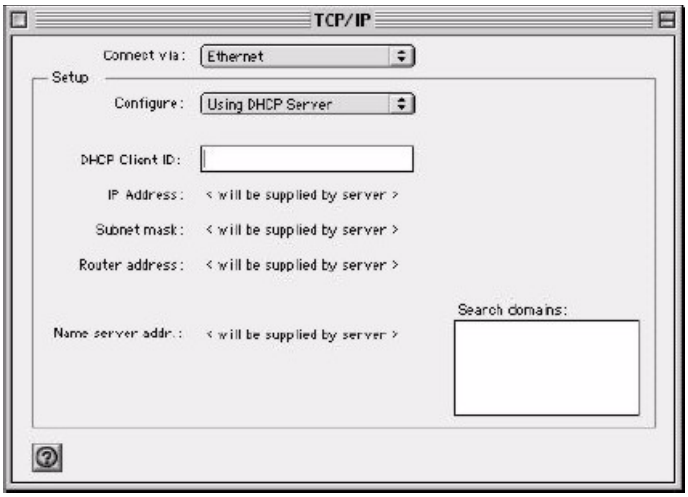
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 189 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 190 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your Prestige and restart your computer (if prompted).

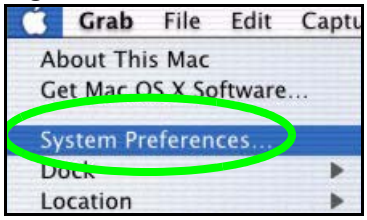
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 191 Macintosh OS X: Apple Menu

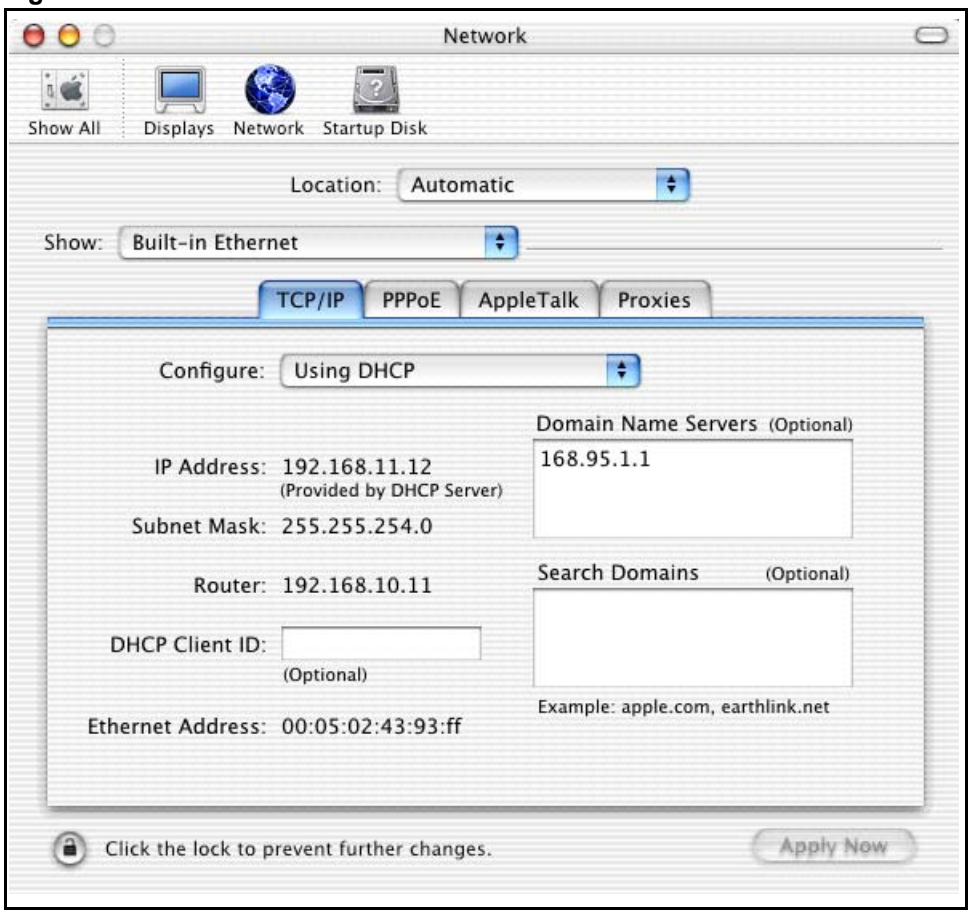


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 192 Macintosh OS X: Network



4 For statically assigned settings, do the following:
   - From the **Configure** box, select **Manually**.
   - Type your IP address in the **IP Address** box.
   - Type your subnet mask in the **Subnet mask** box.
   - Type the IP address of your Prestige in the **Router address** box.
5 Click **Apply Now** and close the window.
6 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

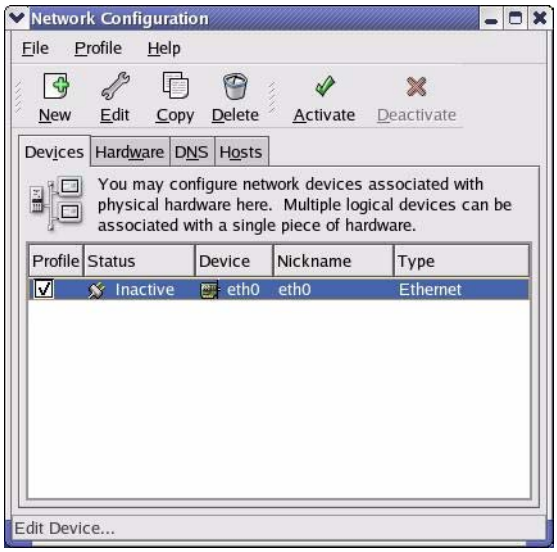
Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 193 Red Hat 9.0: KDE: Network Configuration: Devices



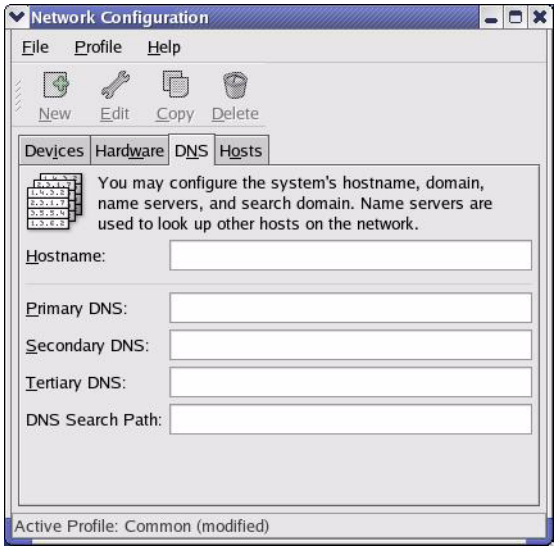
2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

Figure 194 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

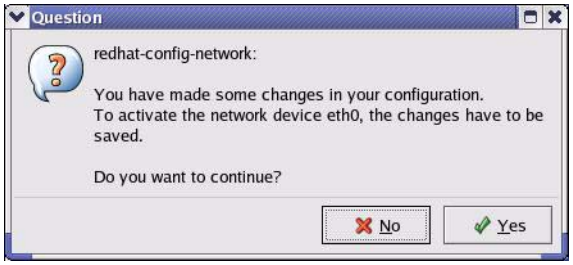
3. Click **OK** to save the changes and close the **Ethernet Device General** screen.
4. If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 195 Red Hat 9.0: KDE: Network Configuration: DNS



5. Click the **Devices** tab.
6. Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 196 Red Hat 9.0: KDE: Network Configuration: Activate


Question
redhat-config-network:
You have made some changes in your configuration.
To activate the network device eth0, the changes have to be saved.
Do you want to continue?
No
Yes

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 197 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 198 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 199 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 200 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

26.6.1 Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 201 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

E

Wireless LANs

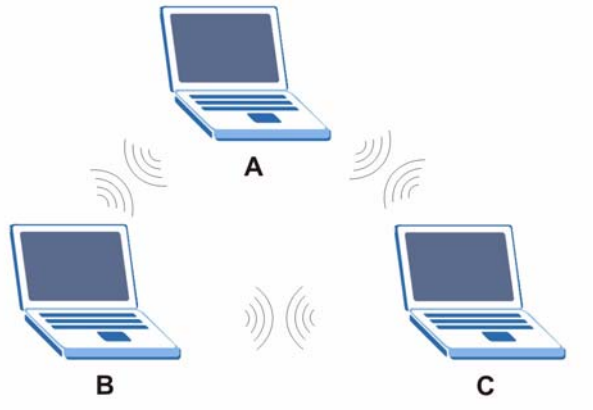
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

Figure 202 Peer-to-Peer Communication in an Ad-hoc Network

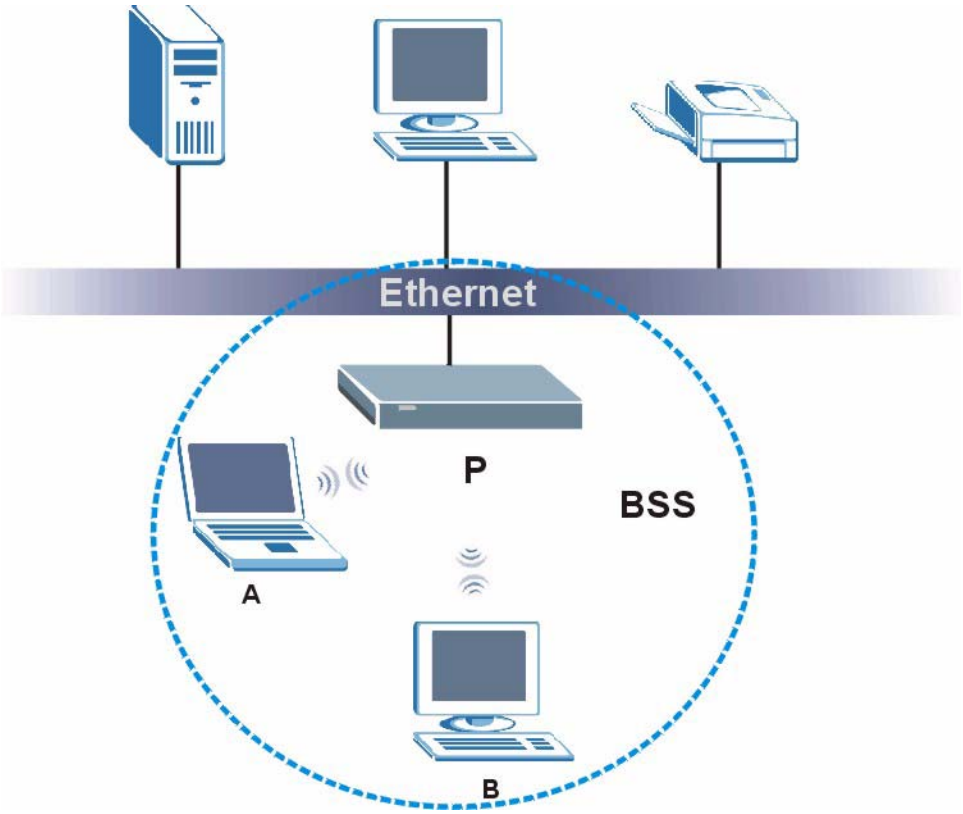


BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 203 Basic Service Set



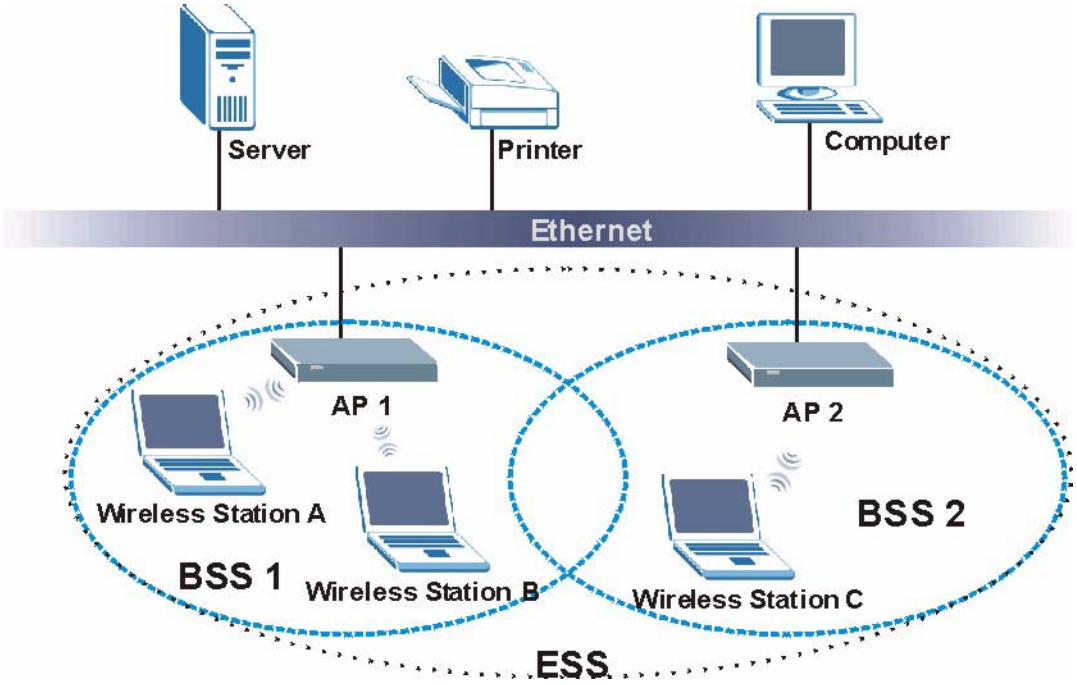
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

Figure 204 Infrastructure WLAN



Channel

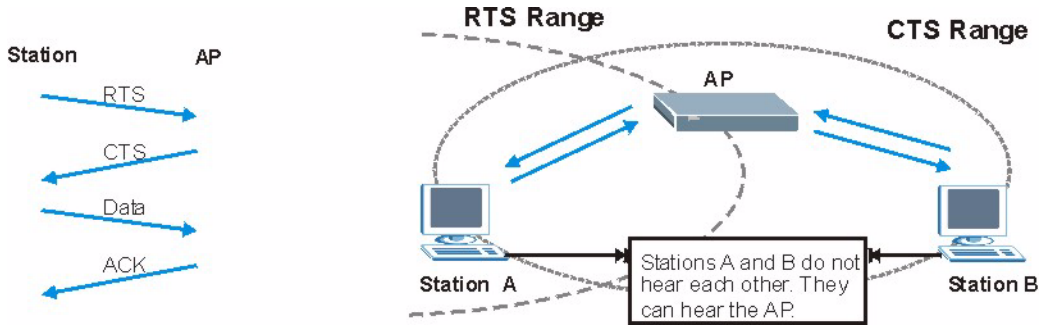
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 205 RTS/CTS



When station A sends data to the AP, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

The AP and the wireless stations MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 128 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
  Determines the identity of the users.
- Authorization
  Determines the network services available to authenticated users once they are connected to the network.
- Accounting
  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless station and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request
  Sent by an access point requesting authentication.
- Access-Reject
  Sent by a RADIUS server rejecting access.
- Access-Accept
  Sent by a RADIUS server allowing access.
- Access-Challenge
  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request
  Sent by the access point requesting accounting.
- Accounting-Response
  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of Authentication

This appendix discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

EAP-MD5 cannot be used with dynamic WEP key exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 129 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA(2)

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA(2) and WEP are improved data encryption and user authentication.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. In addition to TKIP, WPA2 also uses Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

WPA2 AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

User Authentication

WPA or WPA2 applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2 -PSK (WPA2 -Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

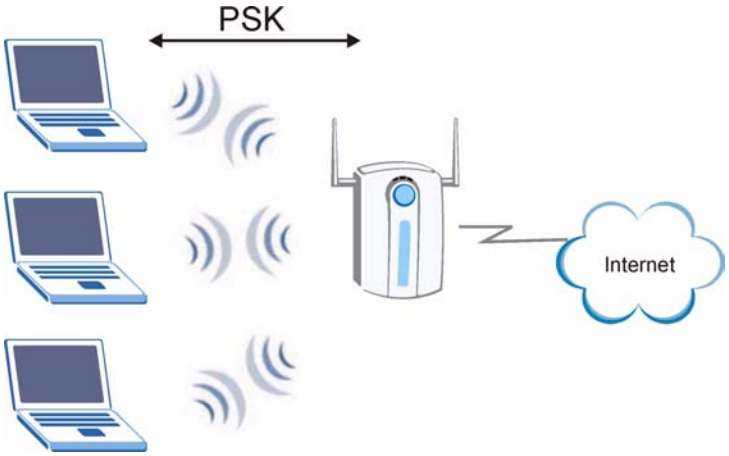
Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

26.6.2 WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
2. The AP checks each wireless client's password and (only) allows it to join the network if the password matches.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

Figure 206 WPA(2)-PSK Authentication



26.6.3 WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 130 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP	No	Enable
WPA-PSK	TKIP	Yes	Enable
WPA2	AES	No	Enable
WPA2-PSK	AES	Yes	Enable

F

Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **User-Defined**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 131 Examples of Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM	TCP	5190	AOL's Internet Messenger service.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.

Table 131 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IMAP4	TCP	143	The Internet Message Access Protocol is used for e-mail.
IMAP4S	TCP	993	This is a more secure version of IMAP4 that runs over SSL.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	The Network Basic Input/Output System is used for communication between computers in a LAN.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S	TCP	995	This is a more secure version of POP3 that runs over SSL.
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.

Table 131 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
ROADRUNNER	TCP/UDP	1026	This is an ISP that provides services mainly for cable modems.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	The Simple File Transfer Protocol is an old way of transferring files between computers.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SMTPS	TCP	465	This is a more secure version of SMTP that runs over SSL.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP	UDP	1900	The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

Table 131 Examples of Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP UDP	7000 user-defined	A videoconferencing solution. The UDP port number is specified in the application.

G

Legal Information

Copyright

Copyright © 2008 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

H

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also http://www.zyxel.com/web/contact_us.php). Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: http://www.zyxel.cn

China - ZyXEL Communications (Shanghai) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-021-61199055
- Fax: +86-021-52069033

- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd., Shanghai
- Web: http://www.zyxel.cn

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Taiwan

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-2-27399889
- Fax: +886-2-27353220
- Web: http://www.zyxel.com.tw
- Address: Room B, 21F., No.333, Sec. 2, Dunhua S. Rd., Da-an District, Taipei

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Turkey

- Support E-mail: cso@zyxel.com.tr
- Telephone: +90 212 222 55 22
- Fax: +90-212-220-2526
- Web: http:www.zyxel.com.tr
- Address: Kaptanpasa Mahallesi Piyalepasa Bulvari Ortadogu Plaza N:14/13 K:6 Okmeydani/Sisli Istanbul/Turkey

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index

A

active protocol 188
AH 188
and encapsulation 189
ESP 188
ActiveX 162
address resolution protocol (ARP) 129
AH 188
and transport mode 189
Alert 234
alternative subnet mask notation 287
any IP
note 129
AP 259
AP (Access Point) 311
AP Mode 259
menu 68
overview 65
status screen 66
AP network 259
Asymmetrical routes 154
and IP alias 154
see also triangle routes 154
authentication algorithms 185, 190
and active protocol 185
Authentication Header. See AH.
Auto-bridge 126

B

Backup configuration 253
Bandwidth management 62
application-based 199
classes and priorities 202
monitor 206
overview 199
priority 200
services 201
subnet-based 199
Bandwidth management monitor 44
Basic wireless security 53
BitTorrent 201
BSS 309

C

CA 315
Certificate Authority 315
certifications 325
notices 326
viewing 326
Channel 41, 67, 311
Interference 311
channel 89
command interface 33
Configuration
backup 253
reset the factory defaults 254
restore 253
contact information 329
Content Filtering
Days and Times 161
Restrict Web Features 161
Cookies 162
copyright 325
CPU usage 41, 67
CTS (Clear to Send) 312
customer support 329

D

Daylight saving 231
DDNS 147
see also Dynamic DNS
DHCP 45, 133
DHCP server
see also Dynamic Host Configuration Protocol
DHCP client information 135
DHCP client list 135
DHCP server 127, 133
DHCP table 45, 135
DHCP client information
DHCP status
Diffie-Hellman key group 185
Perfect Forward Secrecy (PFS) 189
Dimensions 273
disclaimer 325
DNS 59, 135

DNS server
see also Domain name system
DNS (Domain Name System) 212
DNS Server
For VPN Host 190
DNS server 135
Domain name 51
vs host name. see also system name
Domain Name System 135
duplex setting 42, 68
Dynamic DNS 147
Dynamic Host Configuration Protocol 133
Dynamic WEP Key Exchange 316
DynDNS Wildcard 147

E

EAP Authentication 315
e-mail 105
Encapsulating Security Payload. See ESP.
encapsulation
and active protocol 189
transport mode 188
tunnel mode 188
VPN 188
Encryption 317
encryption 91
and local (user) database 91
key 92
WPA compatible 92
encryption algorithms 185, 190
and active protocol 185
ESP 188
and transport mode 189
ESS 310
ESSID 269
Extended Service Set 310
Extended wireless security 54

F

Factory LAN defaults 127
FCC interference statement 325
feature specifications 275
File Transfer Program 201
Firewall 153
Firewall overview
guidelines 154
ICMP packets 156
network security
Stateful inspection 153
ZyXEL device firewall 153
Firmware upload 251
file extension
using HTTP
firmware version 40, 67
Fragmentation Threshold 312
FTP 33, 212
FTP. see also File Transfer Program 201

G

gateway 196
General wireless LAN screen 94

H

Hidden Node 311
HTTP 201
Hyper Text Transfer Protocol 201

I

IANA 292
IBSS 309
IEEE 802.11g 313
IGMP 117, 128
see also Internet Group Multicast Protocol
version
IGMP version 117, 128
IKE SA
aggressive mode 166, 187
authentication algorithms 185, 190
Diffie-Hellman key group 185
encryption algorithms 185, 190
ID content 186
ID type 186
IP address, remote IPSec router 167
IP address, ZyXEL Device 166
local identity 186
main mode 166, 187
NAT traversal 188
negotiation mode 166
peer identity 186
pre-shared key 186
proposal 185

SA life time 190
IKE SA. See also VPN.
Independent Basic Service Set 309
Install UPnP 217
Windows Me 217
Windows XP 218
Internet Assigned Numbers Authority
See IANA
Internet connection
Ethernet
PPPoE. see also PPP over Ethernet
PPTP
WAN connection
Internet connection wizard 54
Internet Group Multicast Protocol 117, 128
Internet Protocol Security. See IPSec.
IP Address 130, 139
IP address 59
dynamic
IP alias 130
IP packet transmission 128
Broadcast
Multicast
Unicast
IP Pool 133
IPSec 165
IPSec SA
active protocol 188
authentication algorithms 185, 190
authentication key (manual keys) 179
encapsulation 188
encryption algorithms 185, 190
encryption key (manual keys) 179
local policy 167
manual keys 179
Perfect Forward Secrecy (PFS) 189
proposal 189
remote policy 167
SA life time 190
Security Parameter Index (SPI) (manual keys) 180
transport mode 188
tunnel mode 188
when IKE SA is disconnected 167, 190
IPSec SA. See also VPN.
IPSec. See also VPN.

J

Java 162

K

Keep alive 190

L

LAN 127
IP pool setup 127
LAN overview 127
LAN Setup 117
LAN setup 127
LAN TCP/IP 127
Language 263
Link type 41, 67
local (user) database 90
and encryption 91
Local Area Network 127
Log 233

M

MAC 101
MAC address 90, 117
cloning 61, 117
MAC address filter 90
MAC address filtering 101
MAC filter 101
managing the device
good habits 33
using FTP. See FTP.
using Telnet. See command interface.
using the command interface. See command interface.
using the web configurator. See web configurator.
Media access control 101
Memory usage 41, 67
Metric 197
MSN messenger 201
MSN Webcam 201
Multicast 117, 128
IGMP 117, 128

N

NAT 137, 139, 292

and VPN 187
overview 137
port forwarding 137
see also Network Address Translation
server sets 137
NAT session 144
NAT Traversal 215
NAT traversal 188
Navigation Panel 42, 68
navigation panel 42, 68
NetBIOS 125, 132
see also Network Basic Input/Output System 125
Network Address Translation 137, 139
Network Basic Input/Output System 132

O

Operating Channel 41, 67

P

P2P 201
peer-to-peer 201
Perfect Forward Secrecy. see PFS.
PFS 189
Diffie-Hellman key group 189
Pocket GUI 108
Point-to-Point Protocol over Ethernet 55, 119
Point-to-Point Tunneling Protocol 56, 122
Pool Size 133
Port forwarding 137, 139
default server 137
example 138
local server 139
port numbers
services
port speed 42, 68
Power Specification 273
PPPoE 55, 119
benefits 56
dial-up connection
see also Point-to-Point Protocol over Ethernet 55
PPTP 56, 122
see also Point-to-Point Tunneling Protocol 56
Preamble Mode 313
priorities 94
Private 197
product registration 327

Q

QoS 94
QoS priorities 94
Quality of Service (QoS) 103

R

RADIUS 314
Shared Secret Key 315
RADIUS Message Types 314
RADIUS Messages 314
RADIUS server 90
registration
product 327
related documentation 3
Remote management 209
and NAT 210
and the firewall 209
FTP 212
limitations 209
remote management session 209
system timeout 210
remote management
Telnet 211
Reset button 39, 254
Reset the device 39
Restore configuration 253
Restrict Web Features 162
RF (Radio Frequency) 274
RFC 2402. See AH.
RFC 2406. See ESP.
RoadRunner 119
Roaming 102
roaming 92
requirements 93
router 259
Router Mode 259
RTS (Request To Send) 312
RTS Threshold 311, 312
RTS/CTS Threshold 103

S

SA
life time 190
safety warnings 6

Scheduling 107
security associations. See VPN.
Security Parameters 319
Service and port numbers 201
Service Set 95
Service Set IDentification 95
Service Set IDentity. See SSID.
services
  and port numbers 321
  and protocols 321
Session Initiated Protocol 201
Simple Mail Transfer Protocol 236
SIP 201
SMTP 236
SNMP 154
SSID 41, 67, 89, 95
Static DHCP 134
Static Route 195
Status 39
subnet 285
Subnet Mask 130
subnet mask 59, 286
subnetting 288
Summary 44
  Bandwidth management monitor 44
  DHCP table 45
  Packet statistics 46
  Wireless station status 47
syntax conventions 4
Sys Op Mode 259
  selecting 260
System General Setup 229
System Name 229
System name 50
  vs computer name
System restart 254

T

TCP/IP configuration 133
Telnet 211
Temperature 273
Time setting 230
trademarks 325
Triangle routes
  and IP alias 154
  see also asymmetrical routes 154
trigger port 142
Trigger port forwarding 142
  example 142
  process 142

U

Universal Plug and Play 215
  Application 215
UPnP 215
  Forum 216
  security issues 215
URL Keyword Blocking 162
Use Authentication 317
user authentication 90
  local (user) database 90
  RADIUS server 90
User Name 148

V

Virtual Private Network. See VPN.
VoIP 201
VPN 80, 122, 165
  active protocol 188
  and NAT 187
  established in two phases 166
  IKE SA. See IKE SA.
  IPSec 165
  IPSec SA. See IPSec SA.
  local network 165
  proposal 185
  remote IPSec router 165
  remote network 165
  security associations (SA) 166
VPN. See also IKE SA, IPSec SA.

W

Wake On LAN 139, 141, 255
WAN
  IP address assignment 58
WAN advanced 125
WAN IP address 58
WAN IP address assignment 60
WAN MAC address 117
warranty 327
  note 327
Web Configurator
  how to access 37

Overview 37
Web configurator
navigating 39
web configurator 33
Web Proxy 162
WEP Encryption 97
WEP encryption 96
WEP key 97
Wi-Fi Multimedia QoS 94
Wildcard 147
Windows Networking 132
Wireless association list 47
wireless channel 269
wireless LAN 269
wireless LAN scheduling 107
Wireless LAN wizard 51
Wireless network
basic guidelines 89
channel 89
encryption 91
example 89
MAC address filter 90
overview 89
security 90
SSID 89
Wireless security 90
overview 90
type 90
wireless security 269
Wireless tutorial 65, 73
WPS 73
Wizard setup 49
Bandwidth management 62
complete 63
Internet connection 54
system information 50
wireless LAN 51
WLAN
Interference 311
Security Parameters 319
WMM 94
WMM priorities 94
WoL. See Wake On LAN.
World Wide Web 201
WPA compatible 92
WPA, WPA2 316
WPS 34
WWW 105, 201

X

Xbox Live 201

Z

ZyNOS 40, 67